

STANDARD STUDENT DATA PRIVACY AGREEMENT

**MASSACHUSETTS, MAINE, ILLINOIS, MISSOURI, NEW HAMPSHIRE, NEW YORK, OHIO,
RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA**

MA-ME-IL-MO-NH-NY-OH-RI-TN-VT-VA-NDPA, Standard Version 1.0

Ontario-Seneca-Yates-Cayuga-Wayne Board of Cooperative Educational Services

(BOCES) and

ASSET PANDA, LLC

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Ontario-Seneca-Yates-Cayuga-Wayne BOCES, located at 131 Drumlin Ct, Newark, NY 14513 USA (the “**Local Education Agency**” or “**LEA**”) and Asset Panda, LLC., located at 5729 Lebanon Road, Ste 144-269 Frisco, Texas 75034 USA (the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - ☒ If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - ☒ If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Jonathan Larkin Title: VP of Operations

Address: 5729 Lebanon Rd Ste 144-269, Frisco, TX 75034

Phone: (855) 898-6058 Email: jonathan@assetpanda.com

The designated representative for the LEA for this DPA is:

Sue Marcano, Sr. Application Support Services Assistant
sue.marcano@edutech.org
131 Drumlin Ct, Newark, NY 14513

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Ontario-Seneca-Yates-Cayuga-Wayne BOCES

By: Kelli Eckdahl Date: 05/28/2025

Printed Name: Kelli Eckdahl Title/Position: Director

Asset Panda, LLC.

By: Jonathan Larkin Date: 2025-05-28

Printed Name: Jonathan Larkin Title/Position: VP of Operations

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data.** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit “F”**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “F”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
 - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
 - (5) In the event of a breach originating from LEA’s use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of

all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

Asset Panda, a cloud-based asset management platform that helps track, manage, and audit physical assets with mobile and web applications.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if Used by Your System
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT “C”

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Student Generated Content: The term “student-generated content” means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline

records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT “F”
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
 - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
 - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
 - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT “G”
Illinois

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Illinois. Specifically, those laws are to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act (“LRA”), 50 ILCS 205; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Illinois;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be replaced with: “This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed.”
2. Replace Notices with: “Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.”
3. In Article II, Section 1, add: “Further clarifying, in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.”
4. In Article II, Section 2, replace “forty-five (45)” with “five (5)”. Add the following sentence: “In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.”

5. In Article II, Section 4, replace it with the following: “In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.”
6. In Article II, Section 5, add: “By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).”
7. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
8. In Article IV, Section 6, replace the whole section with:

The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

9. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
10. In Article IV, Section 7, add “renting,” after “using.”

11. In Article V, Section 1 Data Storage: Illinois requires all Student Data to be stored within the United States.
12. In Article V, Section 4, add the following: “‘Security Breach’ does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.”
13. In Article V, Section 4(1) add the following:
 - vi. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
 - vii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.
14. In Article V, Section 4, add a section (6) which states:

In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

 - a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
 - b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
 - c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

as a result of the security breach; and

 - d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.
15. Replace Article VII, Section 1 with: “In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.”
16. In Exhibit C, add to the definition of Student Data, the following: “Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school

student records", "student temporary record" or "student permanent record" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA."

17. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E:
"The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."
18. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.
19. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.
20. **Student and Parent Access.** Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.
21. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.
22. The Provider will not collect social security numbers.

EXHIBIT “G”

Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
 - a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student’s family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include:
 - i. Details of the incident, including when it occurred and when it was discovered;
 - ii. The type of personal information that was obtained as a result of the breach; and
 - iii. The contact person for Provider who has more information about the incident.
 - b. “*Breach*” shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
 - c. “*Personal information*” is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
 - i. Social Security Number;
 - ii. Driver’s license number or other unique identification number created or collected by a government body;
 - iii. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - v. Medical information; or
 - vi. Health insurance information.

EXHIBIT "G"

Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
6. Provider will not access or monitor any of the following:
 - a. Location-tracking features of a school-issued device;
 - b. Audio or visual receiving, transmitting or recording features of a school-issued device;
 - c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT “G”
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
 1. The credit reporting agencies
 2. Remediation service providers
 3. The attorney general
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student’s ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student’s requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT “G”
Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq.*, T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq.*, T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq.*; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
4. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
5. The Provider agrees that it will not collect individual student data on:
 - a. Political affiliation;
 - b. Religion;
 - c. Voting history; and
 - d. Firearms ownership

EXHIBIT "G"

Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT “G”
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
4. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
 - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
 - (2) Limit unsuccessful logon attempts;
 - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
 - (4) Authorize wireless access prior to allowing such connections;
 - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
 - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
 - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
 - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
 - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
 - (10) Perform maintenance on organizational systems;
 - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
 - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
 - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
 - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
 - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
 - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Exhibit "G"
New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to “Student Data” shall be amended to include and state, “Student Data and APPR Data.”
7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA’s Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor’s Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.
8. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and it’s subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **“Directive for Disposition of Data”** form, a copy of which is attached hereto as **Exhibit “D”**, or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **“Exhibit D”**.

11. To amend Article IV, Section 7 to add: ‘Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, “which term shall not include students.”
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days’ notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider’s facilities, staff, agents and LEA’s Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department’s Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider’s expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider’s privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
 - vi. The number of records affected, if known; and
 - vii. A description of the investigation undertaken so far; and
 - viii. The name of a point of contact for Provider.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.
- (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- “Provider” is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit “C” the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.
-

Exhibit "J"
LEA Documents

LEA's Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy for this service agreement can be accessed at:

https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=12409

Exhibit "K"
Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at

See Attached

Appendix I: Asset Panda Security Documentation

1. Access Control Policy
2. Asset Management Policy
3. Asset Panda Organizational Access Control Policy
4. Business Continuity Plan
5. Code of Conduct
6. Cryptography Policy
7. Data Management Policy
8. Disaster Recovery Plan
9. Human Resource Security Policy
10. Incident Response Plan
11. Information Security Policy – AUP
12. Information Security Roles and Responsibilities
13. Operations Security Policy
14. Physical Security Policy
15. Risk Management Policy
16. Secure Development Policy
17. Third-Party Management Policy



Access Control Policy

CONFIDENTIAL

Do not copy or distribute without permission



Access Control Policy

Policy Owner: Jonathan Larkin

Effective Date: August 17, 2022

Purpose

To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.

Scope

All Asset Panda information systems that process, store, or transmit confidential data as defined in the Asset Panda Data Management Policy are in scope. This policy applies to all employees of Asset Panda and to all external parties with access to Asset Panda engineering networks and system resources.

Policy

Access to information computing resources is limited to personnel with a business requirement for such access. Access rights shall be granted or revoked in accordance with this Access Control Policy.

Business Requirements of Access Control

Access Control Policy

Asset Panda shall determine the type and level of access granted to individual users based on the “principle of least privilege.” This principle states that users are only granted the level of access absolutely required to perform their job functions and is dictated by Asset Panda’s business and security requirements. Permissions and access rights not expressly granted shall be, by default, prohibited.

Asset Panda’s primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC). Wherever feasible, rights and restrictions shall be allocated to groups organized by functions. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production systems should use Multi-Factor Authentication (MFA).



Access to Networks and Network Services

The following security standards shall govern access to Asset Panda networks and network services:

- Technical access to Asset Panda networks must be formally documented including the standard role or approver, grantor, and date
- Only authorized Asset Panda employees and third-parties working off a signed contract or statement of work, with a business need, shall be granted access to the Asset Panda production networks
- Remote connections to production systems and networks must be encrypted

User Access Management

Asset Panda requires that all personnel have a unique user identifier for system access, and that user credentials and passwords are not shared between multiple personnel. Users with multiple levels of access (e.g. administrators) should be given separate accounts for normal system use and for administrative functions wherever feasible. Root, service, and administrator accounts may use a password management system to share passwords for business continuity purposes only. Administrators shall only use shared administrative accounts as needed.

User Registration and Deregistration

Only authorized administrators shall be permitted to create new user IDs, and may only do so upon receipt of a documented request from authorized parties. User provisioning requests must include approval from data owners or Asset Panda management authorized to grant system access. Prior to account creation, administrators should verify that the account does not violate any Asset Panda security or system access control policies such as segregation of duties, fraud prevention measures, or access rights restrictions.

User IDs shall be promptly disabled or removed when users leave the organization or contract work ends. User IDs shall not be re-used.

User Access Provisioning

- New employees and/or contractors are not to be granted access to any Asset Panda production systems until after they have completed all HR on-boarding tasks, which may include but is not limited to signed employment agreement, intellectual property agreement, and information security policy
- Access should be restricted to only what is necessary to perform job duties
- No access may be granted earlier than the official employee start date
- Access requests and rights modifications shall be documented in an access request ticket or email. No permissions shall be granted without approval from the system or data owner or management



- Records of all permission and privilege changes shall be maintained for no less than one year

Management of Privileged Access

The granting of administrative rights shall be strictly controlled and requires approval from the asset owner.

User Access Reviews

Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented.

Access reviews may include group membership as well as evaluations of any specific or exception-based permission. Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.

Removal & Adjustment of Access Rights

The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours.

Access Provisioning, Deprovisioning, and Change Procedure

The Access Management Procedure for Asset Panda systems can be found in Appendix A to this policy.

User Responsibility for the Management of Secret Authentication Information

Controlling and management of individual user passwords is the responsibility of all Asset Panda personnel and third-party users. Users shall protect secret authentication information in accordance with the Information Security Policy.

Password Policy

Where feasible, passwords for confidential systems shall be configured for at least twelve (12) characters with complexity (upper, lower, symbols and numbers).



System and Application Access

Information Access Restriction

Applications must restrict access to program functions and information to authorized users and support personnel in accordance with the defined access control policy. The level and type of restrictions applied by each application should be based on the individual application requirements, as identified by the data owner. The application-specific access control policy must also conform to Asset Panda policies regarding access controls and data management.

Prior to implementation, evaluation criteria are to be applied to application software to determine the necessary access controls and data policies. Assessment criteria include, but are not limited to:

- Sensitivity and classification of data.
- Risk to the organization of unauthorized access or disclosure of data
- The ability to, and granularity of, control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel
- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention and aging features

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all Asset Panda systems, devices, and infrastructure prior to deployment. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, and Simple Network Management Protocol (SNMP) community strings where feasible.

Secure Log-on Procedures

Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and access control architecture.

Password Management System

Systems for managing passwords should be interactive and assist Asset Panda personnel in maintaining password standards by enforcing password strength criteria including minimum length, and password complexity where feasible.



All storage and transmission of passwords is to be protected using appropriate cryptographic protections, either through hashing or encryption.

Use of Privileged Utility Programs

Use of utility programs, system files, or other software that might be capable of overriding system and application controls or altering system configurations must be restricted to the minimum personnel required. Systems are to maintain logs of all use of system utilities or alteration of system configurations. Extraneous system utilities or other privileged programs are to be removed or disabled as part of the system build and configuration process.

Management approval is required prior to the installation or use of any ad hoc or third-party system utilities.

Access to Program Source Code

Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled in order to prevent the introduction of unauthorized functionality into software, avoid unintentional changes, and protect Asset Panda intellectual property.

All access to source code shall be based on business needs and must be logged for review and audit.

Exceptions

Requests for an exception to this Policy must be submitted to the Director of Engineering for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	August 17, 2022	First Version	Jeff McNulty	Suresh Sirigineedi



1.0	August 30, 2023	Policy Review - Updated Policy Owner from Suresh Sirigneedi to Jonathan Larkin	Jeff McNulty	Jonathan Larkin
1.0	September 24, 2024	Policy Review – No changes	Jeff McNulty	Jonathan Larkin



APPENDIX A – Access Management Procedure

At the completion of the onboarding process, HR will send an email that will generate a series of service tickets for access.

HR will provision access for all company-wide systems as well as engineering systems for the Engineering group.

Additional access, beyond standard pre-approved access, must be requested and approved by a manager or system owner.

The access provisioning procedures can be found here:

<https://teamassetpanda.atlassian.net/l/cp/uFQfwhEF>



Asset Management Policy

CONFIDENTIAL

Do not copy or distribute without permission

Asset Management Policy

Policy Owner: Suresh Sirigineedi

Effective Date: June 10, 2022

Purpose

To identify organizational assets and define appropriate protection responsibilities. To ensure that information receives appropriate protection in accordance with its importance to the organization. To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

Scope

This policy applies to all Asset Panda owned or managed information systems.

Policy

Inventory of Assets

Assets associated with information and information processing facilities that store, process, or transmit classified information shall be identified and an inventory of these assets shall be drawn up and maintained.

Ownership of Assets

Assets maintained in the inventory shall be owned by a specific individual or group within Asset Panda.

Acceptable Use of Assets

Rules for the acceptable use of information, assets, and information processing facilities shall be identified and documented in the Information Security Policy.

Return of Assets

All employees and third-party users of Asset Panda equipment shall return all of the organizational assets within their possession upon termination of their employment, contract, or agreement.

Handling of Assets

Employees and users who are issued or handle Asset Panda equipment are expected to use reasonable judgment and exercise due care in protecting and maintaining the equipment.

Employees are responsible for ensuring that company equipment is secured and properly attended to whenever it is transported or stored outside of company facilities.

All mobile devices shall be handled in accordance with the Information Security Policy.

Exceptions

Requests for an exception to this policy must be submitted to the Director of Engineering for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	June 10, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	June 16, 2023	Policy Review - No Changes	Jeff McNulty	Suresh Sirigineedi
1.0	September 24, 2024	Policy Review – Minor grammatical updates based on Microsoft Word recommendations. Changed Policy Owner from Suresh Sirigineedi to Jonathan Larkin	Jeff McNulty	Jonathan Larkin



Access Control Policy

CONFIDENTIAL

Do not copy or distribute without permission



Access Control Policy

Policy Owner: Jonathan Larkin

Effective Date: August 17, 2022

Purpose

To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.

Scope

All Asset Panda information systems that process, store, or transmit confidential data as defined in the Asset Panda Data Management Policy are in scope. This policy applies to all employees of Asset Panda and to all external parties with access to Asset Panda engineering networks and system resources.

Policy

Access to information computing resources is limited to personnel with a business requirement for such access. Access rights shall be granted or revoked in accordance with this Access Control Policy.

Business Requirements of Access Control

Access Control Policy

Asset Panda shall determine the type and level of access granted to individual users based on the “principle of least privilege.” This principle states that users are only granted the level of access absolutely required to perform their job functions and is dictated by Asset Panda’s business and security requirements. Permissions and access rights not expressly granted shall be, by default, prohibited.

Asset Panda’s primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC). Wherever feasible, rights and restrictions shall be allocated to groups organized by functions. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production systems should use Multi-Factor Authentication (MFA).



Access to Networks and Network Services

The following security standards shall govern access to Asset Panda networks and network services:

- Technical access to Asset Panda networks must be formally documented including the standard role or approver, grantor, and date
- Only authorized Asset Panda employees and third-parties working off a signed contract or statement of work, with a business need, shall be granted access to the Asset Panda production networks
- Remote connections to production systems and networks must be encrypted

User Access Management

Asset Panda requires that all personnel have a unique user identifier for system access, and that user credentials and passwords are not shared between multiple personnel. Users with multiple levels of access (e.g. administrators) should be given separate accounts for normal system use and for administrative functions wherever feasible. Root, service, and administrator accounts may use a password management system to share passwords for business continuity purposes only. Administrators shall only use shared administrative accounts as needed.

User Registration and Deregistration

Only authorized administrators shall be permitted to create new user IDs, and may only do so upon receipt of a documented request from authorized parties. User provisioning requests must include approval from data owners or Asset Panda management authorized to grant system access. Prior to account creation, administrators should verify that the account does not violate any Asset Panda security or system access control policies such as segregation of duties, fraud prevention measures, or access rights restrictions.

User IDs shall be promptly disabled or removed when users leave the organization or contract work ends. User IDs shall not be re-used.

User Access Provisioning

- New employees and/or contractors are not to be granted access to any Asset Panda production systems until after they have completed all HR on-boarding tasks, which may include but is not limited to signed employment agreement, intellectual property agreement, and information security policy
- Access should be restricted to only what is necessary to perform job duties
- No access may be granted earlier than the official employee start date
- Access requests and rights modifications shall be documented in an access request ticket or email. No permissions shall be granted without approval from the system or data owner or management



- Records of all permission and privilege changes shall be maintained for no less than one year

Management of Privileged Access

The granting of administrative rights shall be strictly controlled and requires approval from the asset owner.

User Access Reviews

Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented.

Access reviews may include group membership as well as evaluations of any specific or exception-based permission. Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.

Removal & Adjustment of Access Rights

The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours.

Access Provisioning, Deprovisioning, and Change Procedure

The Access Management Procedure for Asset Panda systems can be found in Appendix A to this policy.

User Responsibility for the Management of Secret Authentication Information

Controlling and management of individual user passwords is the responsibility of all Asset Panda personnel and third-party users. Users shall protect secret authentication information in accordance with the Information Security Policy.

Password Policy

Where feasible, passwords for confidential systems shall be configured for at least twelve (12) characters with complexity (upper, lower, symbols and numbers).



System and Application Access

Information Access Restriction

Applications must restrict access to program functions and information to authorized users and support personnel in accordance with the defined access control policy. The level and type of restrictions applied by each application should be based on the individual application requirements, as identified by the data owner. The application-specific access control policy must also conform to Asset Panda policies regarding access controls and data management.

Prior to implementation, evaluation criteria are to be applied to application software to determine the necessary access controls and data policies. Assessment criteria include, but are not limited to:

- Sensitivity and classification of data.
- Risk to the organization of unauthorized access or disclosure of data
- The ability to, and granularity of, control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel
- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention and aging features

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all Asset Panda systems, devices, and infrastructure prior to deployment. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, and Simple Network Management Protocol (SNMP) community strings where feasible.

Secure Log-on Procedures

Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and access control architecture.

Password Management System

Systems for managing passwords should be interactive and assist Asset Panda personnel in maintaining password standards by enforcing password strength criteria including minimum length, and password complexity where feasible.



All storage and transmission of passwords is to be protected using appropriate cryptographic protections, either through hashing or encryption.

Use of Privileged Utility Programs

Use of utility programs, system files, or other software that might be capable of overriding system and application controls or altering system configurations must be restricted to the minimum personnel required. Systems are to maintain logs of all use of system utilities or alteration of system configurations. Extraneous system utilities or other privileged programs are to be removed or disabled as part of the system build and configuration process.

Management approval is required prior to the installation or use of any ad hoc or third-party system utilities.

Access to Program Source Code

Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled in order to prevent the introduction of unauthorized functionality into software, avoid unintentional changes, and protect Asset Panda intellectual property.

All access to source code shall be based on business needs and must be logged for review and audit.

Exceptions

Requests for an exception to this Policy must be submitted to the Director of Engineering for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	August 17, 2022	First Version	Jeff McNulty	Suresh Sirigineedi



1.0	August 30, 2023	Policy Review - Updated Policy Owner from Suresh Sirigneedi to Jonathan Larkin	Jeff McNulty	Jonathan Larkin
1.0	September 24, 2024	Policy Review – No changes	Jeff McNulty	Jonathan Larkin



APPENDIX A – Access Management Procedure

At the completion of the onboarding process, HR will send an email that will generate a series of service tickets for access.

HR will provision access for all company-wide systems as well as engineering systems for the Engineering group.

Additional access, beyond standard pre-approved access, must be requested and approved by a manager or system owner.

The access provisioning procedures can be found here:

<https://teamassetpanda.atlassian.net/l/cp/uFQfwhEF>



Business Continuity Plan

CONFIDENTIAL

Do not copy or distribute without permission

Business Continuity Plan

Policy Owner: [REDACTED]

Effective Date: May 27, 2022

Purpose

The purpose of this business continuity plan is to prepare Asset Panda in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events) and to restore services to the widest extent possible in a minimum time frame.

Scope

All Asset Panda IT systems that are business critical fall in the scope of this policy. This policy applies to all employees of Asset Panda and to all relevant external parties, including but not limited to Asset Panda consultants and contractors.

The following scenarios are excluded from the BC/DR plan scope:

- Loss of availability for a production hosting service provider (i.e., AWS, MongoDB)

In the event of a loss of availability of a hosting service provider, the Director of Engineering will confer with the Operations Managers and executive staff to determine an appropriate response strategy.

Policy

In the event of a major disruption to production services and a disaster affecting the availability and/or security of the Asset Panda application, senior managers and executive staff shall determine mitigation actions.

A disaster recovery test, including a test of backup restoration processes, shall be performed annually.

Continuity of information security shall be considered along with operational continuity.

In the case of an information security event or incident, refer to the Asset Panda Incident Response Plan.

Communications and Escalation

Executive staff and senior managers should be notified of any disaster affecting Asset Panda facilities or operations.

Communications shall take place over any available regular channels, including Slack, email, phone, and online meeting tools.

Business Continuity Plan Key Contacts are as follows:

Name	Role	Position	Email	Phone Number
Support Team	First Line of Communication	Support		
	Recovery Lead	Director of Engineering		
	Coordinator	VP of Operations		
		CFRO		
	CEO	CEO		

Roles and Responsibilities

Name	Position	Responsibility
Recovery Lead	Director of Engineering	<p>The Recovery Lead shall lead BC/DR efforts to mitigate losses and recovery of information systems.</p> <p>The Director of Engineering shall be responsible for leading efforts to maintain continuity of Asset Panda services to customers during a disaster.</p>
Coordinator	VP of Operations CFRO	<p>The coordinator shall be responsible for communications with their departmental staff and any actions needed to maintain continuity of their business functions.</p> <p>Departmental Coordinators shall communicate regularly with executive staff and the Recovery Lead/Director of Engineering and Software Development.</p>
CEO	CEO	<p>The Operation Manager, in conjunction with the CEO, shall be responsible for any external and client communications regarding any disaster or business continuity actions that are relevant to customers and third parties.</p>

Continuity of Critical Services

Strategy for maintaining continuity of services can be seen in the following table:

KEY BUSINESS PROCESS	CONTINUITY STRATEGY
Customer (Production) Service Delivery	Rely on AWS and MongoDB availability commitments and SLAs
IT Operations	Not dependent on physical offices. Critical data is backed up in AWS to alternate regions.
Email	Utilize O365 and its distributed nature, rely on Microsoft's standard service level agreements.
Finance, Legal and HR	All systems are vendor-hosted SaaS applications. Rely on vendor's standard service level agreements.
Sales and Marketing	All systems are vendor-hosted SaaS applications. Rely on vendor's standard service level agreements.

Plan Activation

This Business Continuity Plan shall be automatically activated in the event of a major disruption to production services and a disaster affecting the availability and/or security of the Asset Panda application

Version	Date	Description	Author	Approved by
1.0	May 27, 2022	First Version		
1.1	August 14, 2023	Changed Policy Owner from to Updated 's Tel. #. Added Alt # for Updated Position for		
1.1	September 30, 2024	Policy Review – No Changes		



Code of Conduct

CONFIDENTIAL

Do not copy or distribute without permission

Code of Conduct

Policy Owner: Danielle Kandler

Effective Date: June 10, 2022

Purpose

The primary goal of Asset Panda's Code of Conduct is to foster inclusive, collaborative, and safe working conditions for all Asset Panda staff. As such, Asset Panda are committed to providing a friendly, safe, and welcoming environment for all staff, regardless of gender, sexual orientation, ability, ethnicity, socioeconomic status, and religion (or lack thereof).

This code of conduct outlines our expectations for all Asset Panda staff, as well as the consequences for unacceptable behavior.

Scope

The Code of Conduct applies to all Asset Panda staff. This includes full-time, part-time and contractor staff employed at every seniority level. The Code of Conduct is to be upheld during all professional functions and events, including but not limited to business hours at Asset Panda, during Asset Panda-related extracurricular activities and events, while attending conferences and other professional events on behalf of Asset Panda, and while working remotely and communicating on Asset Panda resources with other staff.

We expect all Asset Panda staff to abide by this Code of Conduct in all business matters -- online and in-person -- as well as in all one-on-one communications with customers and staff pertaining to Asset Panda business.

This Code of Conduct also applies to unacceptable behavior occurring outside the scope of business activities when such behavior can adversely affect the safety and well-being of Asset Panda staff and clients.

Culture and Citizenship

A supplemental goal of this Code of Conduct is to increase open citizenship by encouraging participants to recognize the relationships between our actions and their effects within Asset Panda culture.

CONFIDENTIAL

Do not copy or distribute without permission

Be welcoming. We strive to be a company that welcomes and supports people of all backgrounds and identities. This includes, but is not limited to members of any race, ethnicity, culture, national origin, color, immigration status, social and economic class, educational level, sexual orientation, gender identity and expression, age, size, family status, political belief, religion, and mental and physical ability.

Be considerate. Your work at Asset Panda will be used by other people, and you in turn will depend on the work of others. Any decision you take will affect users and colleagues, and you should consider those consequences when making decisions.

Be respectful. Not all of us will agree all the time, but disagreement is no excuse for poor behavior and poor manners. We might all experience some frustration now and then, but we cannot allow that frustration to turn into a personal attack. It is important to remember that a company where people feel uncomfortable or threatened is neither productive nor pleasant. Asset Panda staff should always be respectful when dealing with other personnel and people outside of Asset Panda employment.

Acceptable and Expected Behavior

The following behaviors are expected and requested of all Asset Panda staff:

- Participate in an authentic and active way. In doing so, you contribute to the health and longevity of Asset Panda.
- Exercise consideration and respect in your speech and actions at all times.
- Attempt collaboration before conflict.
- Refrain from demeaning, discriminatory, or harassing behavior and speech.
- Be mindful of your surroundings and of your fellow participants. Alert Asset Panda leaders if you notice a dangerous situation, someone in distress, or violations of this Code of Conduct, even if they seem inconsequential.
- Remember that Asset Panda events may be shared with members of the public and Asset Panda customers; please be respectful to all patrons of these locations at all times.

Unacceptable Behavior

The following behaviors are considered harassment and are unacceptable within our community:

- Violence, threats of violence or violent language directed against another person.

CONFIDENTIAL

Do not copy or distribute without permission

- Sexist, racist, homophobic, transphobic, ableist or otherwise discriminatory jokes and language.
- Posting or displaying sexually explicit or violent material.
- Posting or threatening to post other people's personally identifying information ("doxing").
- Personal insults, particularly those related to gender, sexual orientation, race, religion, or disability.
- Inappropriate photography or recording.
- Inappropriate physical contact. You should have someone's consent before touching them in any manner.
- Unwelcome sexual attention. This includes sexualized comments or jokes; inappropriate touching, groping, and unwelcome sexual advances.
- Deliberate intimidation, stalking or following (online or in person).
- Advocating for, or encouraging, any of the above behavior.
- Repeated harassment of others. In general, if someone asks you to stop, then stop.
- Other conduct which could reasonably be considered inappropriate in a professional setting.

Weapons Policy

No weapons will be allowed at Asset Panda events or in other spaces covered by the scope of this Code of Conduct. Weapons include but are not limited to guns, explosives (including fireworks), and large knives such as those used for hunting or display, as well as any other item used for the purpose of causing injury or harm to others.

Anyone seen in possession of one of these items will be asked to leave immediately and will be subject to punitive action up to and including termination and involvement of law enforcement authorities. Asset Panda staff are further expected to comply with all state and local laws on this matter.

Consequences of Unacceptable Behavior

Unacceptable behavior from any Asset Panda staff, including those with decision-making authority, will not be tolerated.

Anyone asked to stop unacceptable behavior is expected to comply immediately.

If a staff member engages in unacceptable behavior, Asset Panda leadership may take any action deemed appropriate, up to and including suspension or termination.

Reporting Violations

If you are subject to or witness unacceptable behavior, or have any other concerns, please notify an appropriate member of Asset Panda leadership as soon as possible.

It is a violation of this policy to retaliate against any person making a complaint of Unacceptable Behavior or against any person participating in the investigation of (including testifying as a witness to) any such allegation. Any retaliation or intimidation may be subject to punitive action up to and including termination.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Asset Panda management will determine how serious an employee's offense is and take the appropriate action

Responsibility

It is Human Resource's responsibility to ensure this policy is enforced.

Version	Date	Description	Author	Approved by
1.0	June 10, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	June 2, 2023	Policy Review - Updated Policy Owner	Jeff McNulty	Danielle Kandler
1.0	August 14, 2024	Policy Review - No Changes	Jeff McNulty	Danielle Kandler



Cryptography Policy

CONFIDENTIAL

Do not copy or distribute without permission

Cryptography Policy

Policy Owner: Jon Larkin

Effective Date: May 27, 2022

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. This policy establishes requirements for the use and protection of cryptographic keys throughout their entire lifecycle.

Scope

All information systems developed and/or controlled by Asset Panda, LLC, which store or transmit confidential data.

Policy

Asset Panda, LLC shall evaluate the risks inherent in processing and storing data and shall implement cryptographic controls to mitigate those risks where deemed appropriate. Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented. All encryptions shall be performed in accordance with industry standards, including NIST SP 800-57.

For all personal data, Asset Panda, LLC shall consider the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons, and implement appropriate technical and organizational measures surrounding the pseudonymization and encryption of data to ensure a level of security appropriate to the risk.

For all web traffic sent over the public Internet containing confidential, the TLS v1.2 protocol or better must be utilized.

Key Management

Access to keys and secrets shall be tightly controlled in accordance with the Access Control Policy.

The following table includes the recommended usage for cryptographic keys:

Domain	Key Type	Algorithm	Key Length	Max Expiration
Web Certificate	Digital Signature	DSA or RSA PKCS#1	2048 bit	Up to 2 years for normal certificates, up to 10 years for root certificates.
Web Cipher	Encryption	AES	256 bit	N/A
Confidential	Encryption	AES	256 bit	1 Year
Password	Hash	Bcrypt, PBKDF2, or scrypt, ECDH	256 bit+10K Stretch	N/A
Laptop HDD	Encryption	AES	128 or 256 bit	N/A

Exceptions

Requests for an exception to this policy must be submitted to the Director of Engineering for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	27 May 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	30 May 2023	Policy Review – No Changes	Jeff McNulty	Suresh Sirigineedi
1.0	14 Aug 2024	Policy Review – Updated Owner from Suresh Sirigineedi to Jon Larkin	Jeff McNulty	Jon Larkin



Data Management Policy

CONFIDENTIAL

Do not copy or distribute without permission

Data Management Policy

Policy Owner: Jonathan Larkin

Effective Date: August 23, 2022

Purpose

To ensure that information is classified, protected, retained, and securely disposed of in accordance with its importance to the organization.

Scope

All Asset Panda data, information, and information systems.

Policy

Asset Panda classifies data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements.

Information systems and applications shall be classified according to the highest classification of data that they store or process.

Data Classification

To help Asset Panda and its employees easily understand requirements associated with different kinds of information, the company has created three classes of data.

Confidential

Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive. Examples include:

- Customer Data
- Personally identifiable information (PII)
- Company financial and banking data
- Salary, compensation, and payroll information
- Strategic plans
- Incident reports
- Risk assessment reports
- Technical vulnerability reports
- Authentication credentials

- Secrets and private keys
- Source code
- Litigation data

Restricted

Asset Panda proprietary information requiring thorough protection; access is restricted to employees with a “need-to-know” based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise. Examples include:

- Internal policies
- Legal documents
- Meeting minutes and internal presentations
- Contracts
- Internal reports
- Slack messages
- Email

Public

Documents intended for public consumption which can be freely distributed outside Asset Panda. Examples include:

- Marketing materials
- Product descriptions
- Release notes
- External facing policies

Labeling

Confidential data should be labeled “confidential” whenever paper copies are produced for distribution.

Data Handling

Confidential Data Handling

Confidential data is subject to the following protection and handling requirements:

- Access for non-preapproved roles requires documented approval from the data owner
- Access is restricted to specific employees, roles and/or departments
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential Customer Data shall not be used or stored in non-production systems/environments
- Confidential data shall be encrypted in transit over public networks

- Mobile device hard drives containing confidential data, including laptops, shall be encrypted
- Mobile devices storing or accessing confidential data shall be protected by a log-on password or passcode and shall be configured to lock the screen after five (5) minutes of non-use
- Backups shall be encrypted
- Confidential data shall not be stored on personal phones or devices or removable media including USB drives, CD's, or DVD's
- Paper records shall be labeled "confidential" and securely stored and disposed of
- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed
- Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner

Restricted Data Handling

Restricted data is subject to the following protection and handling requirements:

- Access is restricted to users with a need-to-know based on business requirements
- Restricted systems shall not allow unauthenticated or anonymous access
- Transfer of restricted data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the data owner
- Paper records shall be securely stored and disposed of
- Hard drives and mobile devices used to store restricted information must be securely wiped prior to disposal or physically destroyed

Public Data Handling

No special protection or handling controls are required for public data. Public data may be freely distributed.

Data Retention

Asset Panda shall retain data as long as the company has a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived. Data owners, in consultation with legal counsel, may determine retention periods for their data. Retention periods shall be documented in the Data Retention Matrix in Appendix B to this policy.

Data & Device Disposal

Data classified as restricted or confidential shall be securely deleted when no longer needed. Asset Panda shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet Asset Panda requirements for secure data disposal shall be used to store and process restricted or confidential data.

Asset Panda shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of disposal.

Annual Data Review

Management shall review data retention requirements during the annual review of this policy. Data shall be disposed of in accordance with this policy.

Legal Requirements

Under certain circumstances, Asset Panda may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by Asset Panda legal counsel. Such records and information are exempt from any other requirements specified within this Data Management Policy and are to be retained in accordance with requirements identified by the Legal department. All such holds and special retention requirements are subject to annual review with Asset Panda's legal counsel to evaluate continuing requirements and scope.

Policy Compliance

Asset Panda will measure and verify compliance with this policy through various methods, including but not limited to business tool reports, and both internal and external audits.

Exceptions

Requests for an exception to this policy must be submitted to the Director of Engineering for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	August 23, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	August 30, 2023	Policy Review - Updated Policy Owner from Suresh Sirigineedi to Jonathan Larkin	Jeff McNulty	Jonathan Larkin
1.0	September 24, 2024	Policy Review – No Changes	Jeff McNulty	Jonathan Larkin

APPENDIX A – Data Retention and Disposal Procedure

Asset Panda Application:

Asset Panda's Engineering Team is responsible for setting and enforcing the data retention and disposal procedures for the Asset Panda application. Customer PII data within the Asset Panda application shall be automatically deleted within 90 days of contract termination. Example of customer PII data includes:

- Name
- Email address
- Telephone number
- Job Title
- Physical Address
- Payment information
- Device identifiers
- IP addresses and other passively collected information

Employee Devices:

Asset Panda is responsible for collecting employee devices, clearing or disposing of data, and destroying devices or electronic media.

- Employee devices will be collected promptly upon an employee's termination. Remote employees will be sent a shipping label and the return of their device shall be monitored.
- Collected devices will be cleared to be re-provisioned—or removed from stock, Asset Panda will securely erase the device.
- Device images may be retained at the discretion of management for business purposes
- In cases where a device is damaged in a way that Asset Panda cannot access the Recovery Partition to erase the drive, Asset Panda may optionally decide to use an e-Waste server that includes data destruction with a certificate. Asset Panda will keep certificates of destruction on record for one year. Physical destruction can be optional if it is verified that the device is encrypted with Full Disk Encryption, which would negate the risk of data recovery.

Management will review this procedure at least annually.

APPENDIX B – Data Retention Matrix

Data retention matrix can be found at this link:

<https://teamassetpanda.atlassian.net/l/cp/zE6oWV7u>



Disaster Recovery Plan

CONFIDENTIAL

Do not copy or distribute without permission

Policy Owner: Jonathan Larkin

Effective Date: August 22, 2022

Purpose

The purpose of the Disaster Recovery (DR) Plan is to provide guidance on identifying assets critical to business function, dictate steps on how to prepare for a disaster event, return to operational levels after a disaster, defining the DR Team, guidance on testing the DR Plan and guidance for communication to external parties. This DR Plan is modeled after the guidance provided by NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

Scope

The Disaster Recovery Plan must be followed by all workers (employees, contractors, or third parties) performing work for, and handling information of Asset Panda and/or its affiliates or service providers during a disaster event. This Disaster Recovery Plan shall be automatically activated in the event of a disaster as defined in the Scope section.

Disaster Definition

A “disaster” is any event that can cause significant disruption in computer processing capabilities and/or normal business operations for a period of time. An outage may exist when a service providing support to critical business functions fail or it is determined a service cannot be restored before that service becomes vital. This plan provides information for mature handling of any crisis situation, and as the organization grows the plan must grow to include detailed procedures for the following:

- Executives
- Legal
- Investor Relations
- Corporate Communications
- Corporate Administration
- Marketing and Sales
- Human Resources
- Technology management

Policy

In the event of a major disruption to production services and a disaster affecting the availability and/or security of Asset Panda, senior managers and executive staff shall determine mitigation actions.

This policy and all its components are subject to an annual review. During this review, all aspects of this policy will be checked for efficiency and effectiveness against current procedures, industry standards and best practices, as well as past and future possible events. Additionally, this policy will be reviewed as part of the follow-up phase of DR situation to reflect any shortcomings during the DR procedures. A Disaster Recovery Test, including a test of backup restoration processes, shall be performed on an annual basis. Continuity of information security shall be considered along with operational continuity.

In the case of an information security event or incident, refer to the Incident Response Plan.

Communications and Escalation

Executive staff and senior managers should be notified of any disaster affecting Asset Panda's operations.

Communications shall take place over any available regular channels including:

- Slack
- Email
- Phone
- Zoom

Role	Name	Position	Email	Phone
Support Team	Support Team	Support Team		
Recovery Lead		Director of Engineering		
Coordinator		VP of Operations		
Coordinator		CFRO		
CEO		CEO		

Roles and Responsibilities

The Disaster Recovery Team (DRT) will comprise of the following roles:

Role	Responsibility
Chief Executive Officer (CEO)	<ul style="list-style-type: none">• Responsible for advising the Recovery Lead in DR activities• Coordinates communications to any internal and external parties (clients, vendors, media, etc.)
DR Lead	<ul style="list-style-type: none">• Responsible for managing and directing all activities within the DRP• Manage DR program resources• Coordinate stakeholder participation in DR planning to prioritize critical business processes

	<ul style="list-style-type: none"> • Implement DR policies through DR arrangements such as regular data backups; secure data archival; backup restoration and testing; secure on- and off-site storage of backup media; provision of alternative IT processing facilities, etc. • Evaluate overall DRP program and state of readiness • Manage routine DR reporting; draw relevant information from different business units, plans, incidents, disaster, exercises, etc. • Delivers DR training and awareness activities. • Coordinates test/exercise planning and determines any associated compliance requirements and/or other associated issues.
Coordinator	<ul style="list-style-type: none"> • Supports DR Manager in DR operations • Maintain inventories of IT systems and services supporting critical business processes • Assist with drafting DR-related policies, standards, procedures, and guidelines • Perform or support others in identification and management of DR project-related tasks • Assist with creation of budget requests/proposals, business cases, etc. for various DR activities
Support Team	<ul style="list-style-type: none"> • Assists the Coordinator with any actions required for Disaster Recovery

The following diagram will show the leadership structure for the DRT:



Continuity of Critical Services

Strategy for maintaining continuity of services can be seen in the following table:

KEY BUSINESS PROCESS	CONTINUITY STRATEGY
Asset Panda Application	AWS production environment is replicated in a region different from the region where the primary environment is hosted. The database servers use a cluster with three nodes (MongoDB, AWS RDS, Redis) that allows continuous operation of the database in case the primary node goes down.
Backup Servers	Replicated in 2 different regions for failover
Email	Utilize O365 and its distributed nature, rely on Microsoft's standard service level agreement
Salesforce	Rely on Salesforce's service level agreement
Code Base	Utilizes GitHub and relies on GitHub's service level agreement

This section will define criticality levels according to Asset Panda:

Criticality	Potential Business Impact
1	Complete Disruption
2	Major Functionality Gap
3	Significant Affect on Service Deliverables
4	Immediate Inconvenience

The following table will define the Recovery Time Objective and/or Recovery Point Objective:

Asset	Owner	RTO	RPO	Criticality
Asset Panda Application	DR Lead	4 hours	24 hours	1
Backup Servers	DR Lead	30 minutes	N/A	2
Email	Coordinator	8 hours	N/A	3
Salesforce	Coordinator	8 hours	N/A	1

Code Base	DR Lead	4 hours	N/A	1
-----------	---------	---------	-----	---

Plan

The DRP is outlined in a phased approach. The phases begin before a disaster has occurred and end once all applications have been recovered and any lessons learned have been noted.

Preparation Phase

This section describes the process to develop and maintain an effective IT contingency plan. The process presented here is common to all IT systems. Please reference the DR Plan Testing Template in Appendix A. The steps in the process are as follows:

- **Develop the contingency planning policy statement**
 - The contingency planning policy statement should define the organization's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning.
- **Conduct the business impact analysis (BIA)**
 - The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components.
- **Identify preventive controls**
 - In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system.
- **Develop recovery strategies**
 - Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the BIA.
- **Plan testing, training, and exercises**
 - Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively.
- **Plan maintenance**
 - It is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure new information is documented and contingency measures are revised if required.

Activation Phase

The Notification/Activation Phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan. At the completion of the Notification/Activation Phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis. Damage assessment procedures may be unique for the particular system; however, the following areas should be addressed:

- Cause of the emergency or disruption
- Potential for additional disruptions or damage
- Area affected by the emergency

- Inventory and functional status of IT equipment (e.g., fully functional, partially functional, and nonfunctional)
- Type of damage to IT equipment or data (e.g., water damage, fire and heat, physical impact, and electrical surge)
- Items to be replaced (e.g., hardware, software, firmware, and supporting materials)
- Estimated time to restore normal services.

Recovery Phase

Recovery operations begin after the Disaster Recovery Plan has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery phase activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery Phase, the IT system will be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site. Teams with recovery responsibilities should understand and be able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, they can still perform the necessary activities. Procedures should be assigned to the appropriate recovery team and typically address the following actions:

- Notifying internal and external business partners associated with the system
- Obtaining and loading backup media
- Restoring critical operating system and application software
- Restoring system data
- Testing system functionality including security controls
- Connecting system to network or other external systems
- Operating alternate equipment successfully.

Reconstitution Phase

In the Reconstitution Phase, recovery activities are terminated and normal operations are transferred back to the organization's facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements. Once the original or new site is restored to the level that it can support the IT system and its normal processes, the system may be transitioned back to the original or to the new site. Until the primary system is restored and tested, the contingency system should continue to be operated. The Reconstitution Phase should specify teams responsible for restoring or replacing both the site and the IT system. The following major activities occur in this phase:

- Establishing connectivity and interfaces with network components and external systems
- Testing system operations to ensure full functionality
- Backing up operational data on the contingency system and uploading to restored system
- Shutting down the contingency system
- Terminating contingency operations
- Securing, removing, and/or relocating all sensitive materials at the contingency site
- Arranging for recovery personnel to return to the original facility.

These teams should understand and be able to perform their required functions without a paper plan in the event such documentation is unavailable.

Lessons Learned Phase

The importance of the Lessons Learned Phase is the ability to conduct the Planning Phase effectively to ensure that Asset Panda achieves success. During this phase, the DR Lead will schedule a meeting with the DR Team in order to answer questions related to the disaster. Please reference the Lessons Learned Template in Appendix B. The following questions should be answered:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the disaster? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar disaster occurs?
- How could information sharing with other teams have been improved?
- What corrective actions can prevent similar disasters in the future?
- What precursors or indicators should be watched for in the future to detect similar disasters?
- What additional tools or resources are needed to detect, analyze, and mitigate future disasters?

Version	Date	Description	Author	Approved by
1.0	August 22, 2022	First Version		
1.1	August 14, 2023	Updated 's Tel. # Added Alt # for Updated Position for		

Appendix A – Disaster Recovery Plan Testing Template

1. Schedule
 - Planning Sessions
 - Pre-Test Technical Review
 - Debriefing
2. Introduction
 - Preface
 - Scope
 - Recovery Site
 - Primary Test Objectives
 - Secondary Test Objectives
 - Exclusion (if applicable)
 - Test Assumptions
3. Test Teams
 - Identify teams
4. Pre-Test Planning
 - Activities
 - Issues
 - Concerns
5. Test Timeline
 - Planned start and stop time of test and tasks
 - Actual start and stop time of test and tasks (completed during test)
6. Critical Test Checkpoints
 - Activity
 - Recommendation
 - Responsible Party
7. Test Problem Log
 - Document any problems encountered prior to the test
 - Record any deviations from Test Plan
8. Post-Test Activities
 - Highlights
 - Overall Test Results
 - Test Dates
 - Disaster Recovery Back-up Site
 - Local Access Suite
 - Test Participants
 - Test Objectives
 - Primary Test Objectives
 - Secondary Test Objectives
 - Exclusions
 - Timeline
 - Planned task, start and end times and duration
 - Actual task, start and end times
 - Problems Encountered During the Test
 - Problem Log
 - Actual Problem
 - Ownership
 - Target Date for Resolution

- Status
 - Resolution
 - DR Process or Technical
- Problem Summary
- Follow Up to Pre-Test Problems
- Follow Up to Suggestions for Improvement/Recommendations from Last Year's Test
- Detailed Summary and Observations
- Recommendations for Following Annual Test

Appendix B – Disaster Recovery Plan Lessons Learned Template

Disaster Name – Lessons Learned

CONFIDENTIAL Start Date of Incident:

Lessons Learned Author (w/ Contact Information):

Lessons Learned Completed:

1. Disaster Summary

- a. Include Executive Summary of the Incident here.
 - i. General Overview (including date / time of first attack and when / how first detected)
 - ii. Disaster Profile Type
 - iii. Duration
 - iv. Affected systems and employees
 - v. Impacted business units, clients
 - vi. Estimated costs to the business
- b. The main sequence of events.

2. Detailed Sequence of Disaster

Include a detailed sequence of events here, if available. Be sure to add start and finish dates/times.

3. Major Strengths

List aspects discovered during the DR process which were determined to be major strengths. Describe each in detail.

4. Opportunities for Improvement

List all aspects of the DR process which need improvement.

5. Recommendations

List all formal recommendations from the DRT completing the Lessons Learned activity here. All identified opportunities for improvement must be addressed.



Human Resource Security Policy

CONFIDENTIAL

Do not copy or distribute without permission

Human Resource Security Policy

Policy Owner: Danielle Kandler

Effective Date: June 13, 2022

Purpose

To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.

Scope

This policy applies to all employees of Asset Panda, consultants, contractors and other third-party entities with access to Asset Panda production networks and system resources.

Policy

Screening

Background verification checks on Asset Panda personnel shall be carried out in accordance with relevant laws, regulations, and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Background screening shall include criminal history checks unless prohibited by local statute. All third-parties with technical privileged or administrative access to Asset Panda production systems or networks are subject to a background check or requirement to provide evidence of an acceptable background, based on their level of access and the perceived risk to Asset Panda.

Competence Assessment

The skills and competence of employees and contractors shall be assessed by human resources staff and the hiring manager or his or her designees as part of the hiring process. Required skills and competencies shall be listed in job descriptions and requisitions. Competency evaluations may include reference checks, education and certification verifications, technical testing, and interviews.

All Asset Panda employees will undergo an annual performance review which will include an assessment of job performance, competence in the role, adherence to company policies and code of conduct, and achievement of role-specific objectives.

Terms & Conditions of Employment

Company policies and information security roles and responsibilities shall be communicated to employees and third-parties at the time of hire or engagement. Employees and third-parties with access to company or customer information shall sign an appropriate non-disclosure or confidentiality agreement. Contractual agreements shall state responsibilities for information security as needed. Employees and relevant third-parties shall follow all Asset Panda information security policies.

Management Responsibilities

Management shall be responsible for ensuring that information security policies and procedures are reviewed annually, distributed and available, and that employees and contractors abide by those policies and procedures for the duration of their employment or engagement. Annual policy review shall include a review of any linked or referenced procedures, standards or guidelines.

Management shall ensure that information security responsibilities are communicated to individuals, through written job descriptions, policies or some other documented method which is accurately updated and maintained. Compliance with information security policies and procedures and fulfillment of information security responsibilities shall be evaluated as part of the performance review process wherever applicable.

Information Security Awareness, Education & Training

All Asset Panda employees and third-parties with administrative or privileged technical access to Asset Panda production systems and networks shall complete security awareness training at the time of hire and annually thereafter. Management shall monitor training completion and shall take appropriate steps to ensure compliance with this policy. Employees and contractors shall be aware of relevant information security policies and procedures.

Disciplinary Process

Employees and third-parties who violate Asset Panda information security policies shall be subject to the Asset Panda progressive disciplinary process, up to and including termination of employment or contract.

Exceptions

Requests for an exception to this policy must be submitted to the Controller for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Controller. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company policies up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	June 13, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	June 2, 2023	Policy Review – Updated Policy Owner	Jeff McNulty	Danielle Kandler



Incident Response Plan

CONFIDENTIAL

Do not copy or distribute without permission

Incident Response Plan

Policy Owner: [REDACTED]

Effective Date: August 19, 2022

Purpose

This document establishes the plan for managing information security incidents and events and offers guidance for employees or incident responders who believe they have discovered, or are responding to, a security incident.

Scope

This policy covers all information security or data privacy events or incidents.

Definitions

Security Event – An observable occurrence relevant to the confidentiality, availability, integrity, and/or privacy of company-controlled data, systems, or networks.

Security Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Data Breach – The GDPR defines a “personal data breach” in Article 4(12) as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

Incident Reporting & Documentation

Reporting

If an Asset Panda employee, contractor, user, or customer becomes aware of an information security event or incident, possible incident, imminent incident, unauthorized access, policy violation, security weakness, or suspicious activity, then they shall immediately report the information using one of the following communication channels:

- Email security@assetpanda.com information or reports about the event or incident

Reporters should act as a good witness and behave as if they are reporting a crime. Reports should include specific details about what has been observed or discovered.

Severity

Asset Panda Engineering team shall monitor incident and event tickets and shall assign a ticket severity based on the following categories.

S3/S4 - Low and Medium Severity

Issues meeting this severity are simply suspicions or odd behaviors. They are not verified and require further investigation. There is no clear indicator that systems have tangible risk and do not require emergency response. This includes lost/stolen laptop with disk encryption, suspicious emails, outages, strange activity on a laptop, etc.

S2 - High Severity

High severity issues relate to problems where an adversary or active exploitation hasn't been proven yet, and may not have happened, but is likely to happen. This may include lost/stolen laptop without encryption, vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (e.g.: backdoors, malware), malicious access of business data (e.g.: passwords, vulnerability data, payments information), or threats that put any individual at risk of physical harm.

S1 - Critical Severity

Critical issues relate to actively exploited risks and involve a malicious actor. Identification of active exploitation is required to meet this severity category.

Escalation and Internal Reporting

The incident escalation contacts can be found below in Appendix A.

S1 - Critical Severity: S1 issues require immediate notification to VP of Operations and Customer Support Manager.

S2 - High Severity: A support ticket must be created, and the appropriate manager (see S1 above) must also be notified via slack and email with a reference to the ticket number.

S3/S4 - Medium and Low Severity: A support ticket must be created and assigned to the appropriate department for response.

Documentation

All reported security events, incidents, and response activities shall be documented in Jira as tickets and a detailed incident report on Confluence.

A root cause analysis may be performed on all verified S1 security incidents. A root cause analysis report shall be documented and referenced in the incident ticket. The root cause analysis shall be reviewed by the VP of Operations who shall determine if a post-mortem meeting will be called.

Incident Response Process

For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, eradicate the threat, recover system and services, remediate vulnerabilities, and document a post-mortem with the lessons of an incident.

Summary

- Event reported
- Triage and analysis
- Investigation
- Containment & neutralization (short term work)
- Recovery & vulnerability remediation
- Hardening & Detection improvements (lessons learned, long term work)

Detailed

- VP of Operations will manage the incident response effort
- A central “War Room” will be designated, which may be a physical or virtual location (i.e Slack channel)
- A recurring Incident Response Meeting will occur at regular intervals until the incident is resolved.
- Legal and executive staff will be informed as needed

Incident Response Meeting Agenda

- Update Incident Ticket and timelines
- Document new Indicators of Compromise (IOCs)
- Perform investigative Q&A
- Apply emergency mitigations
- Plan long term mitigations
- Document Root Cause Analysis (RCA)
- Additional items as needed

Special Considerations

Internal Issues

Issues where the malicious actor is an internal employee, contractor, vendor, or partner require sensitive handling. The incident manager shall contact the CEO and HR Manager directly and will not discuss with other employees. These are critical issues where follow-up must occur.

Compromised Communications

Incident responders must have Slack messaging arranged before listing themselves as incident members. If there are IT communication risks, an out of band solution will be chosen, and communicated to incident responders via cell phone.

Additional Requirements

- Suspected and reported events and incidents shall be documented.

- Suspected incidents shall be assessed and classified as either an event or an incident.
- Incident response shall be performed according to this plan and any associated procedures.
- All incidents shall be formally documented, and a documented root cause analysis shall be performed. For EU clients, use the [GDPR Incident Logging & Reporting Template](#). For all other clients, use the Incident Collection Form in Appendix C.
- Suspected and confirmed unauthorized access events shall be reviewed by the Incident Response Team. Breach determinations shall only be made by the CEO and legal counsel in coordination with executive management.
- Asset Panda shall promptly and properly notify customers, partners, users, affected parties, and regulatory agencies of relevant incidents or breaches in accordance with Asset Panda policies, contractual commitments (e.g. Data Processing Agreements, Standard Contractual Clauses), and regulatory requirements (e.g. GDPR, EU-US DPF). For GDPR clients, reference the [List of GDPR Countries](#), the [Quick Guide to GDPR Breach Notifications](#), [Guidelines on Personal Data Breach Notification](#), and the [GDPR Notification Requirements Flowchart](#) in Appendix B.
- This Incident Response Plan shall be reviewed and tested at least annually.

Roles & Responsibilities

Every employee and user of any Asset Panda information resource has responsibilities toward the protection of the information assets. The table below establishes the specific responsibilities of the incident responder roles.

Response Team Members

Role	Responsibility
Incident Manager	<p>The Incident Manager is the primary and ultimate decision maker during the response period. The Incident Manager is ultimately responsible for resolving the incident and formally closing incident response actions. See Appendix A for Incident Manager contact information.</p> <p>These responsibilities include:</p> <ul style="list-style-type: none"> • Ensuring the right people from all functions are actively involved at all times • Status updates are communicated to the appropriate persons at regular intervals • Incidents are resolved in the immediate term • Determining necessary follow-up actions • Assigning follow-up activities to the appropriate people • Promptly reporting incident details which may trigger breach reporting, in writing to the VP of Operations.
Incident Response Team (IRT)	<p>The individuals who have been engaged and are actively working on the incident. All members of the IRT will remain engaged in incident response until the incident is formally resolved, or they are formally dismissed by the Incident Manager.</p>
Engineers (Support and Development)	<p>Qualified engineers will be placed into the on-call rotation and may act as the Incident Manager (if primary resources are not available) or a member of the IRT when engaged to respond to an incident. Engineers are responsible for understanding the technologies and components of the information systems, the security controls in place including logging, monitoring, and alerting tools, appropriate communications channels, incident response protocols, escalation procedures, and documentation requirements. When Engineers are engaged in incident response, they become members of the IRT.</p>
Users	<p>Employees and contractors of Asset Panda. Users are responsible for following policies, reporting problems, suspected problems, weaknesses, suspicious activity, and security incidents and events.</p>
Customers	<p>Customers are responsible for reporting problems with their use of Asset Panda services. Customers are responsible for verifying that reported problems are resolved.</p>
Legal Counsel	<p>Responsible, in conjunction with the CEO and executive management, for determining if an incident shall be considered a reportable breach. Counsel shall review and approve in writing all external breach notices before they are sent to any external party.</p>

Executive Management	<p>Responsible, in conjunction with the CEO and legal counsel, for determining if an incident shall be considered a reportable breach. An appropriate company officer shall review and approve in writing all external breach notices before they are sent to any external party.</p> <p>Asset Panda shall seek stakeholder consensus when determining whether a breach has occurred. The Asset Panda CEO shall make a final breach determination in the event that consensus cannot be reached.</p>
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Management Commitment

Asset Panda management has approved this policy and commits to providing the resources, tools and training needed to reasonably respond to identified security events and incidents with the potential to adversely affect the company or its customers.

Exceptions

Requests for an exception to this Policy must be submitted to and authorized by the VP of Operations approval. Exceptions shall be documented.

Violations & Enforcement

Any known violations of this policy should be reported to the VP of Operations. Violations of this policy may result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	August 19, 2022	First Version		
1.0	August 30, 2023	Policy Review - Updated Policy Owner from [REDACTED] [REDACTED] [REDACTED]		
2.0	June 12, 2024	Replaced “Director of Engineering” with “VP of Operations” Under Additional Comments: + Added reference for the List of GDPR Countries + Added reference for the GDPR Incident Logging & Reporting Template + Added reference for the Quick Guide to GDPR Breach Notifications + Added reference for Personal Data Breach Notification + Added Appendix B - GDPR Notification Requirements Flowchart. + Added examples of contractual commitments (e.g. Data Processing Agreements, Standard Contractual Clauses)		

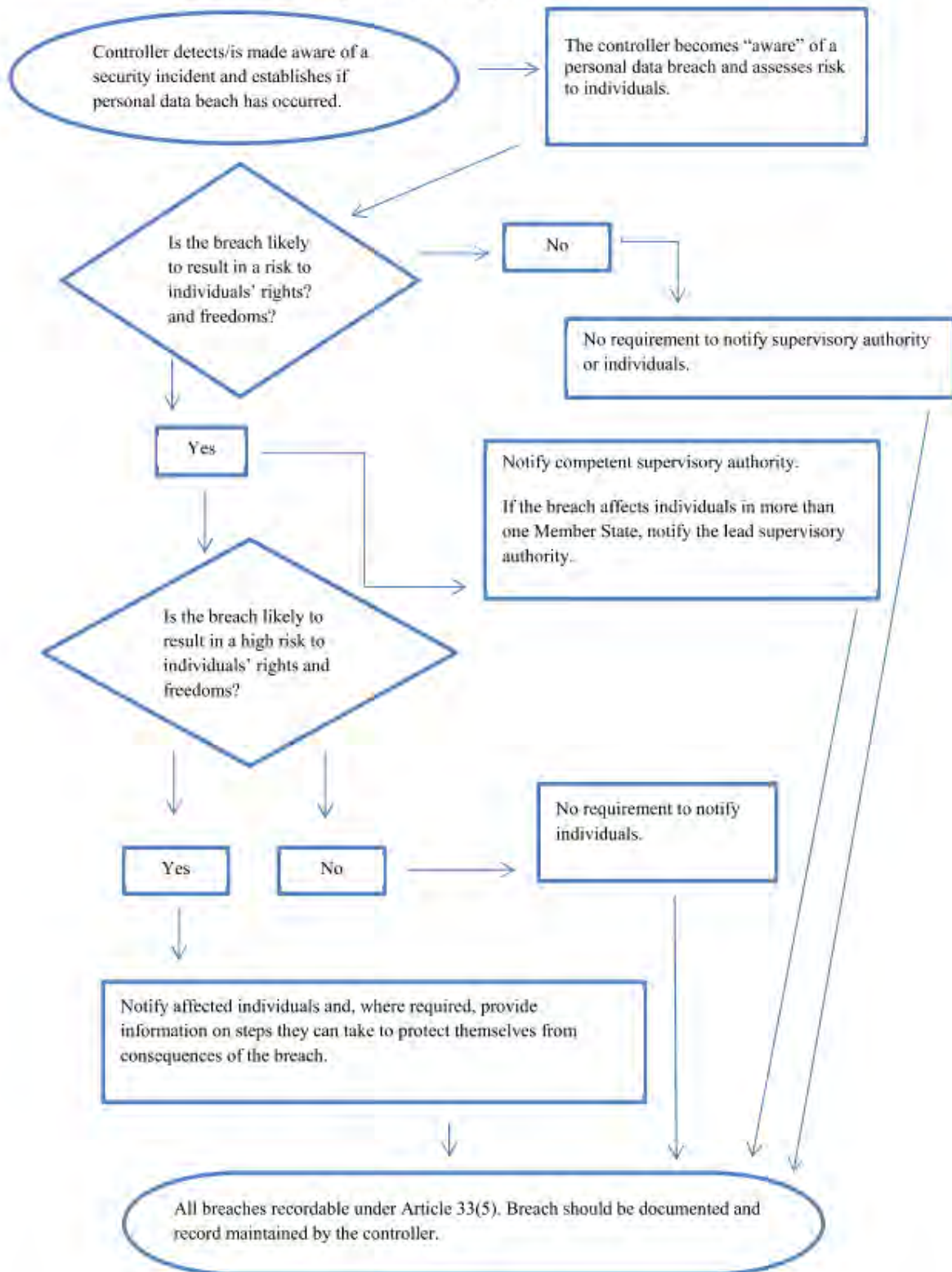
		<ul style="list-style-type: none"> + Added examples of regulatory requirements (e.g. GDPR, EU-US DPF) + Updated definition for Security Incident + Added definition for Data Breach 		
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Appendix A – Contact Information

Contacts for IT and Engineering Management as well as executive staff can be found here at <https://teamassetpanda.atlassian.net/l/cp/qc0BzuJQ>

Appendix B – GDPR Notification Requirements Flowchart

Flowchart showing notification requirements



Appendix C – Incident Collection Form

General Information

Incident Detector's Information

Name:	<input type="text"/>	Date and Time Detected:	<input type="text"/>
Title:	<input type="text"/>		
Phone:	<input type="text"/>	Location Incident Detected From:	<input type="text"/>
E-mail:	<input type="text"/>		
		Additional Information:	<input type="text"/>
			<input type="text"/>
			<input type="text"/>

Incident Summary

Type of Incident Detected:

Denial of Service	Unauthorized Use	Espionage	Probe	Hoax
Malicious Code	Unauthorized Access	Other:		

Incident Location:

Site:	<input type="text"/>
Site Point of Contact:	<input type="text"/>
Phone:	<input type="text"/>
Email:	<input type="text"/>

**How was the Incident
Detected:**

--

Additional Information:

--

Location(s) of affected systems:

--

**Date and time incident handlers arrived
at site:**

--

Describe affected information system(s) (one form per system is recommended):

Hardware Manufacturer:

--

Serial Number:

--

**Corporate Property Number (if
applicable):**

--

**Is the affected system connected to a
network?**

Yes

No

**Describe the physical security of the location of affected information systems (locks, security alarms,
building access, etc.):**

--

--

Isolate affected systems:

Approval to removal from network?

Yes

No

If YES, Name of Approver:

Date and Time Removed:

If NO, state the reason:

Backup of Affected System(s):

Last System backup successful?

Yes

No

Name of persons who did backup:

Date and time last backups started:

Date and time last backups completed:

Backup Storage Location:

Incident Eradication:

Name of persons performing forensics:

Was the vulnerability (root cause) identified:

Yes

No

Describe:

How was eradication validated:



Information Security Policy (AUP)

CONFIDENTIAL

Do not copy or distribute without permission

Information Security Policy

Policy Owner: [REDACTED]

Effective Date: June 10, 2022

Overview

This Information Security Policy is intended to protect Asset Panda's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of Asset Panda. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations.

Effective security is a team effort involving the participation and support of every Asset Panda employee or contractor who deals with information and/or information systems. Every team member is responsible for reading and understanding this policy and conducting their activities accordingly.

Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of Asset Panda's information and assets. These rules are in place to protect customers, employees, and Asset Panda. Inappropriate use exposes Asset Panda to risks including virus attacks, compromise of network systems and services, and legal and compliance issues.

The Asset Panda "Information Security Policy" is comprised of this policy and all Asset Panda policies referenced and/or linked within this document.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Asset Panda business or interact with internal networks and business systems, whether owned or leased by Asset Panda, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Asset Panda and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Asset Panda policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Asset Panda, including all personnel affiliated with third parties. This policy applies to all Asset Panda-controlled companies and customer data as well as all equipment, systems, networks and software owned or leased by Asset Panda.

Security Incident Reporting

All users are required to report known or suspected security events or incidents, including policy violations, and observed security weaknesses. Incidents should be reported immediately or as soon as possible by sending an email to: [REDACTED]

In your email, please describe the incident or observation along with any relevant details.

Mobile Device Policy

All company issued and BYOD end-user devices (e.g., mobile phones, tablets, laptops, desktops) must comply with this policy. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

System level and user level passwords must comply with the Access Control Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All company issued end-user devices used to access Asset Panda information systems (i.e. email) must adhere to the following rules and requirements:

- Devices must be encrypted with a password-protected screensaver or screen lock after 15 minutes of non-use.
- Devices must be locked whenever left unattended
- Users must report any suspected misuse or theft of a mobile device immediately to the Controller
- Confidential information must not be stored on mobile devices or USB drives (this does not apply to business contact information, e.g., names, phone numbers, and email addresses)
- Any mobile device used to access company email must not be shared with any other person
- Upon termination users agree to return all company owned devices and delete all company information and accounts from any personal devices

Remote Access Policy

Laptops and other computer resources that are used to access the Asset Panda network must conform to the security requirements outlined in Asset Panda's Information Security Policies and adhere to the following standards:

- To ensure mobile devices do not connect a compromised device to the company network, Antivirus policies require the use and enforcement of client-side antivirus software

- Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer.
- Users are prohibited from changing or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access Asset Panda resources
- Use of remote access software and/or services (e.g., VPN client) is allowable as long as it is provided by the company and configured for multifactor authentication (MFA)
- Unauthorized remote access technologies may not be used or installed on any Asset Panda system
- Users should use a VPN when transmitting confidential information on public Wi-Fi
- If you access from a public computer (e.g., business center, hotel, etc.), log out of session and don't save anything. Don't check "remember me," collect all printed materials, and delete downloaded files (generally is discouraged) before leaving the computer

Acceptable Use Policy

Asset Panda proprietary and customer information stored on electronic and computing devices whether owned or leased by Asset Panda, the employee or a third party, remains the sole property of Asset Panda for the purposes of this policy. Employees and contractors must ensure through legal or technical means that proprietary information is protected in accordance with the Data Management Policy. The use of One Drive/SharePoint for business file storage is required for users of laptops or company issued devices. Storing important documents on the file share is how you "backup" your laptop.

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Asset Panda proprietary information. You may access, use or share Asset Panda proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company-provided devices.

For security and network maintenance purposes, authorized individuals within Asset Panda may monitor equipment, systems and network traffic at any time.

Asset Panda reserves the right to audit networks and systems periodically to ensure compliance with this policy.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities. Under no circumstances is an employee of Asset Panda authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Asset Panda-owned resources. The list below is not exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Asset Panda.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Asset Panda or the end user does not have an active license.
3. Accessing data, a server, or an account for any purpose other than conducting Asset Panda business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to exporting any material in question.
5. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using an Asset Panda computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
8. Making fraudulent offers of products, items, or services originating from any Asset Panda account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For this section's purposes, "disruption" includes network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Asset Panda engineering team is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the Asset Panda network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means.
17. Providing information about, or lists of: Asset Panda employees, contractors, partners, or customers to parties outside Asset Panda without authorization.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company and act accordingly.

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail", or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Asset Panda networks or other service providers on behalf of, or to advertise, any service hosted by Asset Panda or connected via Asset Panda's network.

Additional Policies and Procedures Incorporated by Reference

Role	Purpose
Access Control Policy	To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.
Asset Management Policy	To identify organizational assets and define appropriate protection responsibilities.
Business Continuity & Disaster Recovery Plan	To prepare Asset Panda in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.
Cryptography Policy	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Data Management Policy	To ensure that information is classified and protected in accordance with its importance to the organization.

Human Resources Policy	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
Incident Response Plan	Policy and procedures for suspected or confirmed information security incidents.
Operations Security Policy	To ensure the correct and secure operation of information processing systems and facilities.
Physical Security Policy	To prevent unauthorized physical access or damage to the organization's information and information processing facilities.
Risk Management Policy	To define the process for assessing and managing Asset Panda's information security risks in order to achieve the company's business and information security objectives.
Secure Development Policy	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.
Third-Party Management Policy	To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

Policy Compliance

Asset Panda will measure and verify compliance with this policy through various methods, including but not limited to business tool reports, and internal and external audits.

Exceptions

Requests for an exception to this policy must be submitted to the Director of Engineering for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	June 10, 2022	First Version	[REDACTED]	[REDACTED]
1.0	August 30, 2023	Policy Review - Updated Policy Owner from [REDACTED] to [REDACTED]	[REDACTED]	[REDACTED]
1.0	September 24, 2024	Policy Review – Minor grammatical updates based on Microsoft Word’s recommendations. No change in policy content.	[REDACTED]	[REDACTED]



Information Security Roles and Responsibilities

CONFIDENTIAL

Do not copy or distribute without permission

Information Security Roles and Responsibilities Policy

Policy Owner: Jon Larkin

Effective Date: June 10, 2022

Statement of Policy

Asset Panda is committed to conducting business in compliance with all applicable laws, regulations, and company policies. Asset Panda has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective

This policy and associated guidance establish the roles and responsibilities within Asset Panda, which is critical for effective communication of information security policies and standards. Roles are required within the organization to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished. Their purpose is to clarify, coordinate activity, and actions necessary to disseminate security policy, standards, and implementation.

Applicability

This policy is applicable to all Asset Panda infrastructure, network segments, and systems.

Audience

The audience for this policy includes all Asset Panda employees and contractors who are involved with the Information Security Program. Awareness of this policy applies for all other agents of Asset Panda with access to Asset Panda information and network. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “Asset Panda community”.

CONFIDENTIAL

Do not copy or distribute without permission

Roles	Responsibilities
Executive Leadership	<ul style="list-style-type: none"> • Oversight over Cyber-Risk and internal control for information security, privacy and compliance • Consults with Executive Leadership to understand Asset Panda IT mission and risks and provides guidance to bring them into alignment • Approves Capital Expenditures for Information Security • Oversight over the execution of the information security risk management program and risk treatments • Communication Path to Asset Panda Director of Engineering • Aligns Information Security Policy and Posture based on Asset Panda's mission, strategic objectives, and risk appetite
Director of Engineering	<ul style="list-style-type: none"> • Oversight over information security in the software development process • Responsible for the design, development, implementation, operation, maintenance and monitoring of development and commercial cloud hosting security controls • Responsible for oversight over policy development • Responsible for implementing risk management in the development process • Oversight over the implementation of information security controls for infrastructure and IT processes • Responsible for the design, development, implementation, operation, maintenance, and monitoring of IT security controls • Ensures IT puts into practice the Information Security Framework • Responsible for conducting IT risk assessments, documenting the identified threats, and maintaining risk register • Communicates information security risks to executive leadership • Reports information security risks annually to Asset Panda's leadership and gains approvals to bring risks to acceptable levels • Coordinates the development and maintenance of information security policies and standards • Works with applicable executive leadership to establish an information security framework and awareness program • Serve as liaison to the Executive Leadership, Law Enforcement, Internal Audit and General Council. • Oversight over Identity Management and Access Control processes
Customer Support Manager	<ul style="list-style-type: none"> • Oversight and implementation, operation and monitoring of information security tools and processes in customer AWS environments • Execution of customer data retention and deletion processes

CONFIDENTIAL

Do not copy or distribute without permission

Systems Owners	<ul style="list-style-type: none"> • Manage the confidentiality, integrity, and availability of the information systems for which they are responsible in compliance with Asset Panda policies on information security and privacy. • Approval of technical access and change requests for non-standard access
Asset Panda Employees, Contractors, temporary workers, etc.	<ul style="list-style-type: none"> • Acting at all times in a manner which does not place at risk the health and safety of themselves, other persons in the workplace, and the information and resources they have use of • Helping to identify areas where risk management practices should be adopted • Taking all practical steps to minimize Asset Panda's exposure to contractual and regulatory liability • Adhering to company policies and standards of conduct • Reporting incidents and observed anomalies or weaknesses
Controller	<ul style="list-style-type: none"> • Ensuring employees and contractors are qualified and competent for their roles • Ensuring appropriate testing and background checks are completed • Ensuring that employees and relevant contractors are presented with company policies and the Code of Conduct (CoC) • Ensuring that employee performance and adherence to the CoC is evaluated at least annually • Ensuring that employees receive appropriate security training • Responsible for oversight over third-party risk management process • Responsible for review of vendor service contracts

Policy Compliance

The Director of Engineering will measure the compliance to this policy through various methods, including, but not limited to—reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the Director of Engineering in advance. Non-compliance will be addressed by management and Human Resources, and can result in disciplinary action in accordance with company procedures up to and including termination of employment.

CONFIDENTIAL

Do not copy or distribute without permission

Version	Date	Description	Author	Approved by
1.0	June 10, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	June 2, 2023	Policy Review, No Changes	Jeff McNulty	Suresh Sirigineedi
1.0	Aug. 14, 2024	Policy Review – Updated Policy Owner from Suresh Sirigineedi to Jon Larkin	Jeff McNulty	Jon Larkin

CONFIDENTIAL

Do not copy or distribute without permission



Operations Security Policy

CONFIDENTIAL

Do not copy or distribute without permission

Operations Security Policy

Policy Owner: Jonathan Larkin

Effective Date: July 6, 2022

Purpose

To ensure the correct and secure operation of information processing systems and facilities.

Scope

All Asset Panda information systems that are business critical and/or process, store, or transmit company data. This Policy applies to all employees of Asset Panda and other third-party entities with access to Asset Panda networks and system resources.

Operations Security

Documented Operating Procedures

Operating procedures shall be documented and made available to all users who need them.

Change Management

Changes to the organization, business processes, information processing facilities, and systems that affect information security in the production environment and financial systems shall be controlled. All significant changes to in-scope systems must be documented.

Change management processes shall include:

- Processes for planning and testing of changes, including remediation measures
- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders
- Documentation of all emergency changes and subsequent review
- A process for remediating unsuccessful changes

Capacity Management

The use of processing resources and system storage shall be monitored and adjusted to ensure that system availability and performance meets Asset Panda requirements.

Human resource skills, availability, and capacity shall be reviewed and considered as a component of capacity planning and as part of the annual risk assessment process.

Scaling resources for additional processing or storage capacity, without changes to the system, can be done outside of the standard change management and code deployment process.

Separation of Development, Staging and Production Environments

Development and staging environments shall be strictly segregated from production SaaS environments to reduce the risks of unauthorized access or changes to the operational environment. Confidential production customer data must not be used in development or test environments without the express approval of the Director of Engineering.

For a full description, see the Data Management Policy for a description of Confidential data. If production customer data is approved for use during development or testing, it shall be scrubbed of any such sensitive information whenever feasible.

Systems and Network Configuration, Hardening, and Review

Systems and networks shall be provisioned and maintained in accordance with the configuration and hardening standards in Appendix A to this policy.

Firewalls shall be used to control network traffic to and from the production environment in accordance with this policy.

Production firewall rules shall be reviewed at least annually. Tickets shall be created to obtain approvals for any needed changes.

Protection from Malware

In order to protect the company's infrastructure against the introduction of malicious software, detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Anti-malware protections shall be utilized on all employee issued laptops except for those running operating systems not normally prone to malicious software. Additionally, threat detection and response software shall be utilized for company email. The anti-malware protections utilized shall be capable of detecting all common forms of malicious threats.

Asset Panda should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download. Anti-malware definition updates should be configured to be downloaded and installed automatically whenever new updates are available. Known or suspected malware incidents must be reported as a security incident.

It is a violation of company policy to disable or alter the configuration of anti-malware protections without authorization.

Information Backup

The need for backups of systems, databases, information and data shall be considered and appropriate backup processes shall be designed, planned and implemented. Security measures to protect backups shall be designed and applied in accordance with the confidentiality or sensitivity of the data. Backup copies of information, software and system images shall be taken regularly to protect against loss of data. Backups and restore capabilities shall be periodically tested, not less than annually.

Asset Panda does not regularly backup user devices like laptops. Users are expected to store critical files and information in company-sanctioned file storage repositories.

Backups are configured to run every 24 hours on in-scope systems. The backup schedules are maintained within the backup application software.

Logging & Monitoring

Production infrastructure shall be configured to produce detailed logs appropriate to the function served by the system or device. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and reviewed through manual or automated processes as needed. Appropriate alerts shall be configured for events that represent a significant threat to the confidentiality, availability or integrity of production systems or Confidential data.

Protection of Log Information

Logging facilities and log information shall be protected against tampering and unauthorized access.

Administrator & Operator Logs

System administrator and system operator activities shall be logged and reviewed and/or alerted in accordance with the system classification and criticality.

Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to network time servers using reputable time sources.

Intrusion Detection

Asset Panda production systems shall be configured to monitor, log, and alert on suspicious changes to critical system files where feasible.

Alerts shall be configured for suspicious conditions and engineers shall review logs on a regular basis.

Unauthorized intrusions and access attempts or changes to Asset Panda systems shall be investigated and remediated in accordance with the Incident Response Plan.

Control of Operational Software

The installation of software on production systems shall follow the change management requirements defined in this policy.

Technical Vulnerability Management

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures taken to address the associated risk. A variety of methods shall be used to obtain information about technical vulnerabilities, including vulnerability scanning, penetration tests, and the bug bounty program.

External vulnerability scans shall be run on the production environment at least quarterly. Interior vulnerability scans shall be run against test environments which mirror production configurations.

Penetration tests of the applications and production network shall be performed at least annually. Additional scanning and testing shall be performed following major changes to production systems.

The Engineering department shall evaluate the severity of vulnerabilities, and if it is determined to be a critical or high-risk vulnerability, a service ticket will be created. The Asset Panda assessed severity level may differ from the level automatically generated by scanning software or determined by external researchers based on Asset Panda's internal knowledge and understanding of technical architecture and real-world impact/exploitability. Tickets are assigned to the system, application, or platform owners for further investigation and/or remediation.

Vulnerabilities assessed by Asset Panda shall be remediated in the following timeframes:

Determined Severity	Remediation Time
Critical	24 Hours
High	30 Days
Medium	60 Day
Low	90 Days
Informational	As needed

Service tickets for any vulnerability which cannot be remediated within the standard timeline must show a risk treatment plan and planned remediation timeline.

Restrictions on Software Installation

Rules governing the installation of software by users shall be established and implemented in accordance with the Asset Panda Information Security Policy.

Information Systems Audit Considerations

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

Exceptions

Requests for an exception to this policy must be submitted to the Director of Engineering for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	June 8, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	August 30, 2023	Updated Policy Owner from Suresh Sirigineedi to Jonathan Larkin	Jeff McNulty	Jonathan Larkin
1.0	September 24, 2024	Annual Review – No Changes	Jeff McNulty	Jonathan Larkin

APPENDIX A - Configuration and Hardening Standards

Configuration and hardening standards shall be maintained on the internal documentation portal.

<https://teamassetpanda.atlassian.net/wiki/home>



Physical Security Policy

CONFIDENTIAL

Do not copy or distribute without permission

Physical Security Policy

Policy Owner: Jon Larkin

Effective Date: June 8, 2022

Purpose

To prevent unauthorized physical access or damage to the organization's information and information processing facilities.

Scope

Asset Panda is a cloud-based SaaS company with no physical office. This Policy applies to all employees of Asset Panda, and to all external parties with physical access to Asset Panda owned or leased facilities.

Policy

Physical Security Perimeter

Asset Panda's perimeter layer security controls are inherited through our cloud provider, Amazon Web Services (AWS). This Layer includes a number of security features, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures. You can learn more about AWS's Perimeter Layer security features at:

<https://aws.amazon.com/compliance/data-center/data-centers/>.

Physical Entry Controls

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Where possible, cloud provider access control systems shall be tied to a centralized system that provides granular access control for individual personnel. Access events shall be appropriately logged and reviewed as needed according to risk. Cameras and intrusion detection systems shall be used at facilities that store or process production data.

Securing Offices, Rooms & Facilities

Physical security for offices, rooms and facilities shall be designed and applied to protect from theft, misuse, environmental threats, unauthorized access, and other threats to the confidentiality, integrity, and availability of classified data and systems.

CONFIDENTIAL

Do not copy or distribute without permission

Protecting Against External & Environmental Threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. Secure areas shall be monitored through the use of intrusion detection systems, alarms, and/or video surveillance systems where feasible. Visitor and third-party access to secure areas shall be restricted to reduce the risk of information loss and theft.

Production processing facilities shall be equipped with appropriate environmental and business continuity controls including fire-suppression systems, climate control and monitoring systems, and emergency backup power systems. Physical information system hardware and supporting infrastructure shall be regularly serviced and maintained in accordance with the manufacturer's recommendations.

Working in Secure Areas / Visitor Management

Visitors, delivery personnel, outside support technicians, and other external agents shall not be permitted access to secure areas without escort and/or appropriate oversight. Third-parties in secure areas shall sign in and out on a visitor log and shall be escorted or monitored by AWS personnel. External party access to secure areas shall be confirmed with appropriate AWS personnel prior to being granted access. AWS personnel providing access to external parties into secure areas are responsible for ensuring that the third-party personnel adhere to all security requirements, and are accountable for all actions taken by outsiders they provide with access. Visitors may be allowed to work unescorted provided that the Asset Panda sponsoring party can ensure that they will not have unauthorized access to Asset Panda information systems, networks, or data.

Delivery & Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter secure areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Supplier, Vendor, and Third-Party Security

Suppliers, vendors, and third-parties shall comply with Asset Panda physical security and environmental controls requirements. Asset Panda shall assess the adequacy of third-party physical security controls as part of the vendor management process, in accordance with the Third-Party Management Policy.

Exceptions

Requests for an exception to this policy must be submitted to the Controller for approval.

CONFIDENTIAL

Do not copy or distribute without permission

Violations & Enforcement

Any known violations of this policy should be reported to the Controller. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	June 8, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	May 30, 2023	Policy Review – No Changes	Jeff McNulty	Suresh Sirigineedi
1.0	Aug 14, 2024	Policy Review – Updated Policy Owner from Suresh Sirigineedi to Jon Larkin	Jeff McNulty	Jon Larkin

CONFIDENTIAL

Do not copy or distribute without permission



Risk Management Policy

CONFIDENTIAL

Do not copy or distribute without permission

Risk Management Policy

Policy Owner: Jon Larkin

Effective Date: June 10, 2022

Purpose

To define the methodology for assessing and managing Asset Panda's information security risks in order to achieve the company's business and information security objectives.

Scope

The risk assessment process may be applied to all business processes, information, information systems, networks, devices, and information processing facilities that are owned or used by Asset Panda applicants, employees, contractors, consultants, vendors, partners, and other users affiliated with Asset Panda, or others using or accessing Asset Panda networks and/or information systems.

Policy

Asset Panda will ensure that risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a risk management policy is designed to ensure that the company achieves its stated business and security goals and objectives.

Risk Management Strategy

Asset Panda has developed processes to identify those risks that would hinder the achievement of its strategic and operational objectives. Asset Panda will therefore ensure that it has in place the means to identify, analyze, control, and monitor the strategic and operational risks it faces using this risk management policy based on best practices.

The Director of Engineering will ensure the risk management strategy and policy are reviewed regularly and that:

- The risk management policy is applied to relevant areas at Asset Panda
- The risk management policy and its operational application are annually reviewed
- Non-compliance is reported to appropriate company officers and authorities

Practical Application of Risk Management

Asset Panda may use a variety of risk reporting formats for the identification of risks, their classification, and evaluation based on factors such as vendors utilized, methodology employed, and the scope of the assessment. In general, and where possible, risks shall be assessed and ranked according to their impact and their likelihood of occurrence. A formal IT risk assessment, network penetration tests, and Asset Panda application penetration test will be performed at least annually.

In addition, an internal audit of the information security management system (ISMS) (i.e., information security controls and management processes) shall be performed at least annually.

Security risks shall be evaluated at various stages of the software design and development lifecycle as needed.

Risk Categories

Some risks are within the control of Asset Panda while others may be only to a lesser degree. Asset Panda will consider the risks within each of the following categories:

- Technical
- Reputational
- Contractual
- Economic/Financial
- Regulatory/Compliance
- Fraud

Each identified risk will be assessed as to its likelihood and impact. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. The likelihood and impact will be considered together to formulate an overall risk ranking.

Risk Criteria

The criteria for determining risk is the combined likelihood and impact of an event adversely affecting the confidentiality, availability, integrity, or privacy of customer data, personally identifiable information (PII), or business critical systems.

For all risk inputs such as risk assessments, penetration tests, vulnerability scans, etc., Asset Panda management shall reserve the right to modify automated or third-party provided risk rankings based on its assessment of the nature and criticality of the system processing, as well as the nature, criticality and exploitability (or other relevant factors and considerations) of the identified vulnerability.

Risk Response and Treatment

Risks will be prioritized and mapped using the approach contained in this policy. The following responses to risk should be employed. Where Asset Panda chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan.

- Mitigate: Asset Panda may take actions or employ strategies to reduce the risk.
- Accept: Asset Panda may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- Transfer: Asset Panda may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Asset Panda, or insurance may be appropriate for protection against financial loss.
- Eliminate: The risk may be such that Asset Panda could decide to cease the activity or to change it in such a way as to end the risk.

Risk Management Procedure

The procedure for managing risk will meet the following criteria:

- Asset Panda will maintain a Risk Register and Treatment Plan.
- Risks shall be ranked by 'likelihood' and 'severity/impact' as critical, high, medium, low, or negligible.
- Overall risk shall be determined through a combination of likelihood and impact.
- Risks may be valued to estimate potential monetary loss where practical, or may be considered relative to a control objective
- Asset Panda will respond to risks in a prioritized fashion. Remediation priority will consider the risk likelihood and impact, cost, work effort, and availability of resources. Multiple remediations may be undertaken simultaneously.
- Periodic reports will be made to the senior leadership of Asset Panda to ensure risks are being mitigated appropriately, and in accordance with business priorities and objectives.

Risk Acceptance Levels

Role	Responsibility
CEO	Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.
Director of Engineering	Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register. This person shall be responsible for communicating risks to top management and the board and adopting risk treatments in accordance with executive direction. Shall be responsible for adherence to this policy.

Amendment & Termination of this Policy

Asset Panda reserves the right to modify, amend or terminate this policy at any time.

Exceptions

Requests for an exception to this Policy must be submitted to the Director of Engineering for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	June 10, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	June 16, 2023	Policy Review - No Changes	Jeff McNulty	Suresh Sirigineedi
1.0	September 30, 2024	Policy Review. Update Policy Owner from Suresh Sirigineedi to Jon Larkin	Jeff McNulty	Jon Larkin

Appendix A: Risk Assessment Matrix and Description Key

	RISK = LIKELIHOOD * IMPACT	LIKELIHOOD		
		Very likely: 3	Somewhat likely: 2	Not likely: 1
IMPACT	Very impactful: 3	9	6	3
	Somewhat impactful: 2	6	4	2
	Not impactful: 1	3	2	1

RISK LEVEL	RISK DESCRIPTION
Low (1–2)	A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.
Moderate (3–6)	A threat event could be expected to have a serious adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.
High (7–9)	A threat event could be expected to have a severe adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.

IMPACT LEVEL	IMPACT DESCRIPTION
Not impactful (1)	A threat event could be expected to have a limited adverse effect, meaning: degradation of mission capability yet primary functions can still be performed; minor damage; minor financial loss; or range of effects is limited to some cyber resources but no critical resources.
Somewhat impactful (2)	A threat event could be expected to have a serious adverse effect, meaning: significant degradation of mission capability yet primary functions can still be performed at a reduced capacity; minor damage; minor financial loss; or range of effects is significant to some cyber resources and some critical resources.
Very impactful (3)	A threat event could be expected to have a severe or catastrophic adverse effect, meaning: severe degradation or loss of mission capability and one or more primary functions cannot be performed; major damage; major financial loss; or range of effects is extensive to most cyber resources and most critical resources.

LIKELIHOOD LEVEL	LIKELIHOOD DESCRIPTION
Not likely (1)	Adversary is unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is unlikely to occur; or threat is unlikely to have adverse impacts.
Somewhat likely (2)	Adversary is somewhat unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is somewhat unlikely to occur; or threat is somewhat unlikely to have adverse impacts.
Very likely (3)	Adversary is highly likely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is highly likely to occur; or threat is highly likely to have adverse impacts.



Secure Development Policy

CONFIDENTIAL

Do not copy or distribute without permission

Secure Development Policy

Policy Owner: Suresh Sirigineedi

Effective Date: August 17, 2022

Purpose

To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Scope

All Asset Panda applications and information systems that are business critical and/or process, store, or transmit Confidential data are in scope. This policy applies to all internal and external engineers and developers of Asset Panda software and infrastructure.

Policy

This policy describes the rules for the acquisition and development of software and systems that shall be applied to developments within the Asset Panda organization.

System Change Control Procedures

Changes to systems within the development lifecycle shall be controlled using formal change control procedures. Change control procedures and requirements are described in the Asset Panda Operations Security Policy.

In accordance with Asset Panda's [Source Code Management Best Practices](#), all code changes shall be reviewed and approved by a minimum of two peers before being merged into any production branch.

Software Version Control

All Asset Panda software shall be version controlled and synced between contributors (developers). Access to the central code repository shall be restricted based on an employee's role. All code shall be written, tested, and saved in a local repository BEFORE being synced to the origin repository.

Technical Review of Applications after Operating Platform Changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.

Restrictions on Changes to Software Packages

Modifications to third-party business application packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

Secure System Engineering Principles

Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system implementation efforts.

Engineering style guides and technical references can be found here: [Coding Style Guides](#)

Software developers shall adhere to Asset Panda's coding standards throughout the development cycle, including standards for quality, commenting, and security.

Secure Development Environment

Asset Panda shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

Outsourced Development

Asset Panda shall supervise and monitor the activity of outsourced system development. Outsourced development shall adhere to all Asset Panda standards and policies.

System Security Testing

Testing of security functionality shall be carried out during development. No code shall be deployed to Asset Panda production systems without documented, successful test results.

System Acceptance Testing

Acceptance testing programs and related criteria shall be established for new information systems, upgrades, and new versions.

Prior to deploying code, a Release Checklist MUST be completed. The Release Checklist shall include a list of all Test Plans and shows the completion of all associated tests.

Protection of Test Data

Test data shall be selected carefully, protected, and controlled. Confidential customer data shall be protected in accordance with all contracts and commitments. Customer data shall not be used for testing purposes without the explicit permission of the data owner and the Director of Engineering.

Acquisition of Third-Party Systems and Software

The acquisition of third-party systems and software shall be done in accordance with the requirements of the Asset Panda Third-Party Management Policy.

Exceptions

Requests for an exception to this Policy must be submitted to the Director of Engineering for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	August 17, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	August 30, 2023	Policy Review – No Changes	Jeff McNulty	Suresh Sirigineedi

1.0	September 30, 2024	Policy Review – No Changes	Jeff McNulty	Suresh Sirigineedi
-----	--------------------	----------------------------	--------------	--------------------



Third-Party Management Policy

CONFIDENTIAL

Do not copy or distribute without permission

Third-Party Management Policy

Policy Owner: Jon Larkin

Effective Date: June 8, 2022

Purpose

To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

This document outlines a baseline of security controls that Asset Panda expects partners and other third-party companies to meet when interacting with Asset Panda Confidential data.

Scope

All data and information systems owned or used by Asset Panda that are business critical and/or process, store, or transmit Confidential data. This policy applies to all employees of Asset Panda and to all external parties, including but not limited to Asset Panda consultants, contractors, business partners, vendors, suppliers, partners, outsourced service providers, and other third-party entities with access to Asset Panda data, systems, networks, or system resources.

Policy

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

For all service providers who may access Asset Panda Confidential data, systems, or networks, proper due diligence shall be performed prior to provisioning access or engaging in processing activities. Information shall be maintained regarding which regulatory or certification requirements are managed by or impacted by each service provider, and which are managed by Asset Panda as required. Applicable regulatory or certification requirements may include ISO 27001, SOC 2, PCI-DSS, CCPA, GDPR or other frameworks or regulations.

Information Security in Third-Party Relationships

Addressing Security in Agreements

Relevant information security requirements shall be established and agreed with each supplier that may access, process, store, or transmit Confidential data, or provide physical or virtual IT infrastructure components for Asset Panda.

For all service providers who may access Asset Panda production systems, or who may impact the security of the Asset Panda production environment, written agreements shall be maintained that include the service provider's acknowledgment of their responsibilities for the confidentiality of company and customer data, and any commitments regarding the integrity, availability, and/or privacy controls that they manage in order to meet the standards and requirements that Asset Panda has established in accordance with Asset Panda's information security program or any relevant framework.

Technology Supply Chain

Asset Panda will consider and assess risk associated with suppliers and the technology supply chain. Where warranted, agreements with suppliers shall include requirements to address the relevant information security risks associated with information and communications technology services and the product supply chain.

Third-Party Service Delivery Management

Monitoring & Review of Third-Party Services

Asset Panda shall regularly monitor, review, and audit supplier service delivery. Supplier security and service delivery performance shall be reviewed at least annually.

Management of Changes to Third-Party Services

Changes to the provision of services by suppliers, including changes to agreements, services, technology, policies, procedures, or controls, shall be managed, taking account of the criticality of the business information, systems, and processes involved. Asset Panda shall assess the risk of any material changes made by suppliers and make appropriate modifications to agreements and services accordingly.

Third-Party Risk Management

Asset Panda will ensure that potential risks posed by sharing Confidential data are identified, documented and addressed according to this policy. Risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a partner and third-party security policy is to ensure that partnerships and services achieve their business plan aims and objectives, and are consistent with Asset Panda's requirements for information security.

Asset Panda shall not share or transmit Confidential data to a third-party without first performing a third-party risk assessment and fully executing a written contract, statement of work or service agreement which describes expected service levels and any specific information security requirements.

Third-Party Security Standards

All third-parties must maintain reasonable organizational and technical controls as assessed by Asset Panda.

Assessment of third-parties which receive, process, or store Confidential data shall consider the following controls as applicable based on the service provided and the sensitivity of data stored, processed or exchanged.

Information Security Policy

Third-parties maintain information security policies supported by their executive management, which are regularly reviewed.

Risk Assessment & Treatment

Third-parties maintain programs that assess, evaluate, and manage information and technology risks.

Operations Security

Third-parties implement commercially reasonable practices and procedures designed, as appropriate, to maintain operations security. Protections may include:

- Technical testing
- Protection against malicious software
- Network protection and management
- Technical vulnerability management
- Logging and monitoring
- Incident response
- Business continuity planning

Access Control

Third-parties maintain a technical access control program.

Secure System Development

Third-parties maintain a secure development program consistent with industry software and systems development best practices including risk assessment, formal change management, code standards, code review and testing.

Physical & Environmental Security

If third-parties are storing or processing confidential data, their physical and environmental security controls should meet the requirements of the Asset Panda Physical Security Policy.

Human Resources

Third-parties maintain human resource policies and processes which include criminal background checks for any employees or contractors who access Asset Panda Confidential information.

Compliance & Legal

Asset Panda shall consider all applicable regulations and laws when evaluating suppliers and third parties who will access, store, process or transmit Asset Panda Confidential data. Third-party assessments should consider the following criteria:

- Protection of customer data, organizational records, and records retention and disposition
- Privacy of Personally Identifiable Information (PII)

Exceptions

Requests for an exception to this Policy must be submitted to the Controller for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Controller. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	June 8, 2022	First Version	Jeff McNulty	Suresh Sirigineedi
1.0	June 16, 2023	Policy Review - No Changes	Jeff McNulty	Suresh Sirigineedi
1.0	September 30, 2024	Policy Review. Updated policy owner from Suresh Sirigineedi to Jon Larkin.	Jeff McNulty	Jon Larkin

Appendix II: Asset Panda SOC 2 Certification

System and Organization Controls (SOC) 2 Type II Report

Report on Controls Placed in Operation and Test of Operating
Effectiveness Relevant to the Trust Services Criteria for
Security Category

For the Period
January 30, 2024 to January 30, 2025

Together with Independent Service
Auditor's Report

Report on Management's Description of



TABLE OF CONTENTS

I. Independent Service Auditor's Report	3
II. Assertion of Asset Panda LLC Management	7
III. Description of Asset Panda	9
IV. Description of Test of Controls and Results Thereof	21



Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Asset Panda LLC

Scope

We have examined Asset Panda LLC's accompanying description of its Asset Panda (system) titled "Description of Asset Panda" throughout the period January 30, 2024 to January 30, 2025 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 30, 2024 to January 30, 2025, to provide reasonable assurance that Asset Panda LLC's service commitments and system requirements were achieved based on trust services criteria relevant to security principles (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Asset Panda LLC uses a subservice organization, to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Asset Panda LLC, to achieve Asset Panda LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Asset Panda LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Asset Panda LLC's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Asset Panda LLC, to achieve Asset Panda LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Asset Panda LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Asset Panda LLC's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Asset Panda LLC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Asset Panda LLC's service commitments and system requirements were achieved. Asset Panda LLC has provided an assertion titled "Assertion of Asset Panda LLC's Management" (assertion) about the description and the suitability of design and operating effectiveness of the controls stated therein. Asset Panda LLC is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description, and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Description of Test of Controls and Results Thereof."

Opinion

In our opinion, in all material respects,

- a. The description presents Asset Panda LLC's Asset Panda (system) that was designed and implemented throughout the period January 30, 2024 to January 30, 2025 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period January 30, 2024 to January 30, 2025, to provide reasonable assurance that Asset Panda LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Asset Panda LLC's controls throughout the period.
- c. The controls stated in the description operated effectively throughout the period January 30, 2024 to January 30, 2025, to provide reasonable assurance that Asset Panda LLC's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Asset Panda LLC's controls operated effectively throughout the period.

Restricted Use

This report, including the description of tests of controls and results thereof in the section of our report titled “Description of Test of Controls and Results Thereof” is intended solely for the information and use of Asset Panda LLC; user entities of Asset Panda LLC’s Asset Panda during some or all of the period January 30, 2024 to January 30, 2025, business partners of Asset Panda LLC subject to risks arising from interactions with the Asset Panda LLC’s processing system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization’s system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity’s ability to effectively use the service organization’s services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Johanson Group LLP

Colorado Springs, Colorado
March 12, 2025



Section II

ASSERTION OF ASSET PANDA LLC MANAGEMENT

We have prepared the accompanying description of Asset Panda LLC's "Description of Asset Panda" for the period January 30, 2024 to January 30, 2025, (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Asset Panda LLC's Asset Panda (system) that may be useful when assessing the risks arising from interactions with Asset Panda LLC's system, particularly information about system controls that Asset Panda LLC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Asset Panda LLC uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Asset Panda LLC, to achieve Asset Panda LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Asset Panda LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Asset Panda LLC's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Asset Panda LLC, to achieve Asset Panda LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Asset Panda LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Asset Panda LLC's controls.

We confirm, to the best of our knowledge and belief, that:

- a. The description presents Asset Panda LLC's Asset Panda (system) that was designed and implemented throughout the period January 30, 2024 to January 30, 2025, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period January 30, 2024 to January 30, 2025, to provide reasonable assurance that Asset Panda LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Asset Panda LLC's controls throughout that period.
- c. The controls stated in the description operated effectively throughout the period January 30, 2024 to January 30, 2025, to provide reasonable assurance that Asset Panda LLC's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Asset Panda LLC's controls operated effectively throughout that period.

Asset Panda LLC Management
March 12, 2025



Section III

DESCRIPTION OF ASSET PANDA

COMPANY BACKGROUND

Asset Panda is a SaaS company headquartered in Frisco, TX that offers a cloud-based, highly configurable solution for streamlining asset tracking, inventory management, vendor management, and a wide variety of other processes for thousands of companies in hundreds of industries.

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

The Asset Panda Platform provides customers with a full lifecycle tracking solution for assets. The system description in this section of the report details the Asset Panda Platform. Any other Asset Panda services are not within the scope of this report.

Asset Panda is a highly configurable SaaS platform that can be accessed with desktops, laptops, tablets, and mobile devices through both a web application and mobile apps. The system is cloud-based and enables our clients to track assets, manage inventory, create tickets, perform audits, manage facilities, and configure notifications for events.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Asset Panda LLC designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Asset Panda LLC makes to user entities, the laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Asset Panda LLC has established for the services. The system services are subject to the security commitments established internally for its services.

Asset Panda's commitments to users are communicated through Service Level Agreements (SLAs) or Master Service Agreements (MSAs), online Privacy Policy, online Terms of Use, and in the description of the service offering provided online.

Security Commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Uptime availability of production systems

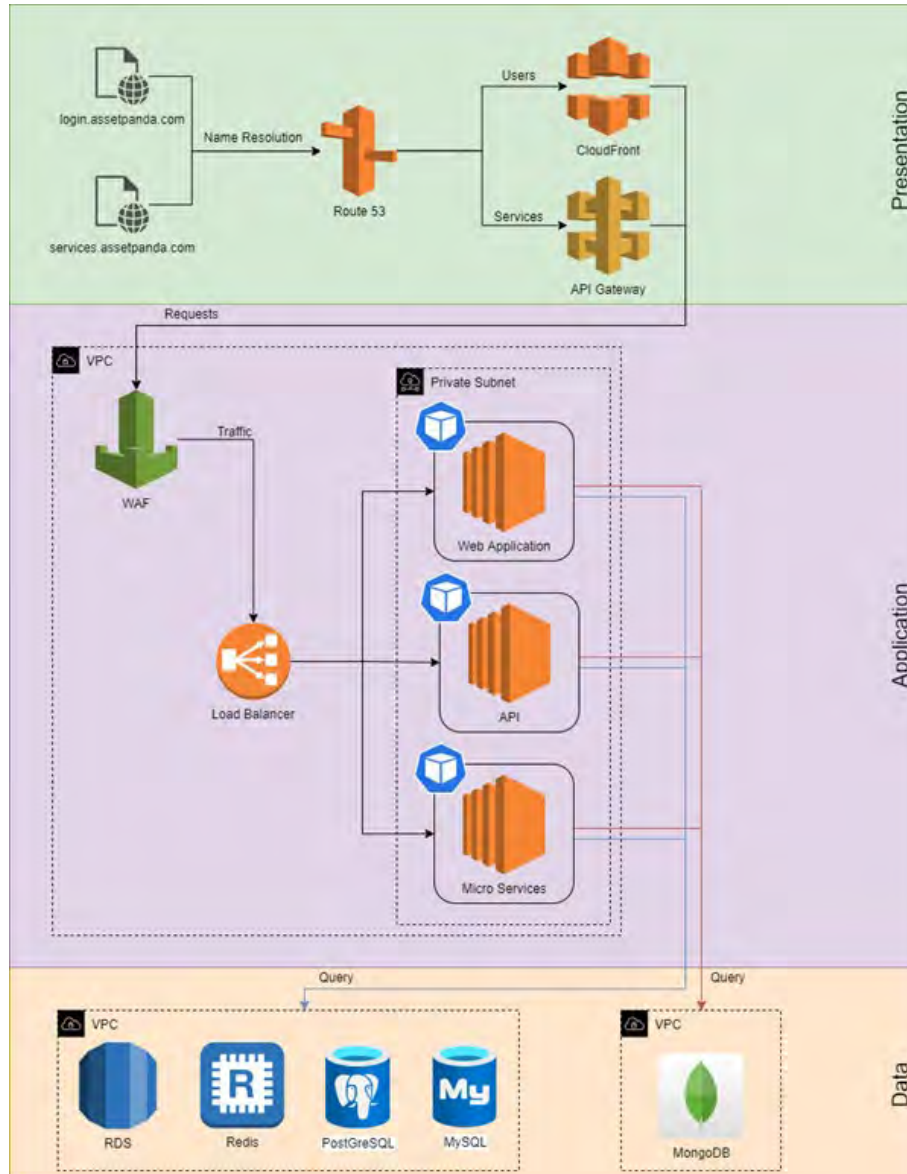
COMPONENTS OF THE SYSTEM

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

Asset Panda LLC maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, inventory type, description, and owner. To outline the topology of its network, the organization maintains the following network diagram(s).



Primary Infrastructure		
Hardware	Type	Purpose
AWS Elastic Compute Cloud (EC2)	AWS	Compute
AWS Elastic Load Balancers	AWS	Load balances internal and external traffic.
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access.
S3 Buckets	AWS	Storage, upload, and download.

Software

Asset Panda LLC is responsible for managing the development and operation of the Asset Panda system, including infrastructure components such as servers, databases, and storage systems. The in-scope Asset Panda LLC infrastructure and software components are shown in the table provided below:

Primary Software		
System/Application	Operating System	Purpose
GuardDuty	AWS	Security application used for automated intrusion detection (IDS).
Datadog	Datadog	Monitoring application used to provide monitoring, alter, and notification services for Asset Panda LLC platform.
PostgreSQL	Linux	Transactional database
Redis	Linux	Used to maintain cached data.
MongoDB	Linux	Used for storing the assets database.

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Asset Panda LLC has a staff of approximately 58 organized in the following functional areas:

- **Management:** Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

This includes:

- CEO - Rex Kurzius
 - CFRO - Justin Lackey
 - VP of Operations - Jonathan Larkin
 - VP of Product - Ram Shamanna
 - Director of Engineering - Suresh Sirigineedi
 - HR Generalist – Danielle Kandler
 - Manager of Organizational Development & Customer Support - Kelly Donaldson
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality. Responsible for managing access to production, staging, and development environments for the application.
- **Operations:** Responsible for maintaining the availability and functionality of internal tools, including some production tools. Manages access and security for production infrastructure in partnership with the HR and Engineering teams. Only members of the Operations and Engineering teams have administrative access to the production environment. Members of the Operations team may also be members of the Engineering team.
- **Information Technology:** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations. Responsible for provisioning email and security-related accounts for the onboarding of new employees.
- **Product:** Responsible for identifying customer needs in coordination with Marketing, Sales, and Customer Success teams, and designing solutions for those needs. This involves everything from existing product enhancements to full new product ideation. The Engineering team handles requests from the Product team to develop and bring solutions to the market.

- **Human Resources:** Responsible for onboarding and offboarding employees in our workforce management system and active directory, which supplies data to our access monitoring systems. Responsible for requesting access to systems during the onboarding process, but does not have the ability to provide access to any back-end tools.
- **Finance:** Responsible for managing accounting, record keeping, cash flow, and reporting of financial-related matters throughout the organization.
- **Marketing:** Responsible for demand generation for the product and identifying market needs for potential expansion opportunities and product direction. Produces marketing materials, manages the marketing website, maintains overall product branding, and develops go-to-market strategies to expand our client base.
- **Sales:** Responsible for serving the needs of inbound prospects to sell Asset Panda products to meet the new business generation goals for the organization. Creates trial accounts for potential customers and hands new clients to the Implementation team to complete new account configurations.
- **Implementation:** Responsible for onboarding clients after they purchase Asset Panda's products, including account configuration and initial training for new clients.
- **Training & Support:** Responsible for providing ongoing training to employees on security compliance, internal and external systems, and job effectiveness. Also responsible for providing support to Asset Panda clients when they encounter problems with using the application.

Data

Data as defined by Asset Panda LLC, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service, GDPR, and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized into the following major types of data used by Asset Panda LLC.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Asset Panda LLC.	<ul style="list-style-type: none"> • Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	<ul style="list-style-type: none"> • Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Asset Panda LLC. Asset Panda LLC must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	<ul style="list-style-type: none"> • Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Asset Panda LLC to operate the business. Asset Panda LLC must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	<ul style="list-style-type: none"> • Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured and utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, protect customer data. Additionally, Asset Panda LLC has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

Asset Panda LLC's production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Asset Panda LLC reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical Access

Asset Panda LLC provides employees and contractors access to infrastructure via a role-based access control system to ensure uniform, least privileged access to identified users and to maintain simple and repeatable user provisioning and de-provisioning processes.

Access to these systems is split into admin roles, user roles, and no-access roles. User access and roles are reviewed on a quarterly basis to ensure the least privileged access.

Management is responsible for providing access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Asset Panda LLC's policies and completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Management is responsible for de-provisioning access to all in-scope systems within 3 days of that employee's termination.

Computer Operations – Backups

Customer data is backed up and monitored by the Engineering for completion and exceptions. If there is an exception, Engineering will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations – Availability

Asset Panda LLC maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Asset Panda LLC internally monitors all applications, including the web UI, databases, and cloud storage, to ensure that service delivery matches SLA requirements.

Asset Panda LLC utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Change Management

Asset Panda LLC maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Asset Panda LLC has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Asset Panda LLC application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and de-provisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

Asset Panda uses an automated monitoring service to perform quarterly vulnerability scans and engages an external firm to perform annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

BOUNDARIES OF THE SYSTEM

The boundaries of the Asset Panda are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Asset Panda.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security Category)
<p>Security refers to the protection of</p> <ol style="list-style-type: none"> information during its collection or creation, use, processing, transmission, and storage, and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Asset Panda LLC's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Asset Panda LLC's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Asset Panda LLC's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated the required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The Asset Panda LLC management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Asset Panda LLC can help customers build data workflows, as well as new security technologies that can help protect those workflows and any regulatory changes that may require Asset Panda LLC to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Asset Panda LLC's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Asset Panda LLC's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Asset Panda LLC's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. Asset Panda LLC's human resources policies and practices relating to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

Asset Panda LLC's risk assessment process identifies and manages risks that could potentially affect Asset Panda LLC's ability to provide reliable and secure services to our customers. As part of this process, Asset Panda LLC maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Asset Panda LLC product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Asset Panda LLC's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Asset Panda LLC addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Asset Panda LLC's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATIONS SYSTEMS

Information and communication are an integral component of Asset Panda LLC's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Asset Panda LLC uses several information and communication channels internally to share information with management, employees, contractors, and customers. Asset Panda LLC uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Asset Panda LLC uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Asset Panda LLC's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Asset Panda LLC's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Asset Panda LLC's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Asset Panda LLC's personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

INCIDENTS

No significant incidents have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All Common Security Criteria were applicable to Asset Panda LLC's Asset Panda system.

SUBSERVICE ORGANIZATIONS

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Subservice Description of Services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entity's services.

Complementary Subservice Organization Controls

Asset Panda LLC's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Asset Panda LLC's services to be solely achieved by Asset Panda LLC control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Asset Panda LLC.

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

Subservice Organization - AWS		
Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed-circuit television cameras (CCTVs) are used to monitor server locations in data centers. Images are retained for 90 days unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.

Asset Panda LLC management, along with the subservice provider, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Asset Panda LLC performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports.
- Testing controls performed by vendors and subservice organization(s).
- Reviewing attestation reports over services provided by vendors and subservice organization(s).
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization(s).

COMPLEMENTARY USER ENTITY CONTROLS

Asset Panda LLC's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Asset Panda LLC's services to be solely achieved by Asset Panda LLC control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Asset Panda LLC.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Asset Panda LLC.
2. User entities are responsible for notifying Asset Panda LLC of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Asset Panda LLC services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Asset Panda LLC services.
6. User entities are responsible for providing Asset Panda LLC with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Asset Panda LLC of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.



Section IV

DESCRIPTION OF TEST OF CONTROLS AND
RESULTS THEREOF

Relevant trust services criteria and Asset Panda LLC-related controls are an integral part of management's system description and are included in this section. Johanson Group LLP performed testing to determine if Asset Panda LLC's controls were suitably designed and operating effectively to achieve the specified criteria for the security category set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*, throughout the period January 30, 2024 to January 30, 2025.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Asset Panda LLC activities and operations, and inspection of Asset Panda LLC documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Johanson LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Asset Panda LLC controls, this test was not listed individually for every control in the tables below.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
Control Environment			
CC 1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Inspected Asset Panda LLC's sample of completed background checks to determine that the company performs it on new employees.	No exceptions noted.
	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected Asset Panda LLC's sample of contractor agreements to determine that the company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	No exceptions noted.
	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected Asset Panda LLC's Code of Conduct to determine that the company requires employees to acknowledge a policy at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	No exceptions noted.
	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected Asset Panda LLC's sample of contractor agreements to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected Asset Panda LLC's sample of a signed confidentiality agreement to determine that the company requires employees to sign a confidentiality agreement during onboarding.	No exceptions noted.
	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected Asset Panda LLC's sample of completed performance evaluations to determine that company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
CC 1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company management demonstrates a commitment to integrity and ethical values.	Inspected Asset Panda LLC's ethical management questionnaire to determine that the company management demonstrates a commitment to integrity and ethical values.	No exceptions noted.
CC 1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected Asset Panda LLC's Security Policies to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected Asset Panda LLC's organization chart to determine that the company maintains a chart that describes the organizational structure and reporting lines.	No exceptions noted.
	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Asset Panda LLC's Information Security Roles and Responsibilities to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
CC 1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Asset Panda LLC's Information Security Roles and Responsibilities to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
	The company performs background checks on new employees.	Inspected Asset Panda LLC's sample of completed background checks to determine that the company performs it on new employees.	No exceptions noted.
	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected Asset Panda LLC's sample of completed performance evaluations to determine that company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected Asset Panda LLC's sample of completed security awareness training records to determine that the company requires employees to complete the training within thirty days of hire and at least annually thereafter.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
CC 1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Asset Panda LLC's Information Security Roles and Responsibilities to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected Asset Panda LLC's Code of Conduct to determine that the company requires employees to acknowledge a policy at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	No exceptions noted.
	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected Asset Panda LLC's sample of completed performance evaluations to determine that company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
Communication and Information			
CC 2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected Asset Panda LLC's continuous security monitoring in Vanta to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	No exceptions noted.
	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected Asset Panda LLC's log management tool to determine that the company utilizes a system to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
CC 2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected Asset Panda LLC's whistleblower policy to determine that the company has established an anonymous communication channel is in place for users to report potential issues or fraud concerns.	No exceptions noted.
	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected Asset Panda LLC's Security Policies to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Asset Panda LLC's Information Security Roles and Responsibilities to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected Asset Panda LLC's information security policies and procedures to determine that they are documented and reviewed at least annually.	No exceptions noted.
	The company communicates system changes to authorized internal users.	Inspected Asset Panda LLC's internal communication for system updates to determine that the company communicates system changes to authorized internal users.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected Asset Panda LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company provides a description of its products and services to internal and external users.	Inspected Asset Panda LLC's network diagram and product documentation to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected Asset Panda LLC's sample of completed security awareness training records to determine that the company requires employees to complete the training within thirty days of hire and at least annually thereafter.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
CC 2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	Inspected Asset Panda LLC's public change log or release notes to determine that the company notifies customers of critical system changes that may affect their processing.	No exceptions noted.
	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected Asset Panda LLC's customer support site or email alias to determine that the company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected Asset Panda LLC's MSA template and publicly available terms of service to determine that the company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	No exceptions noted.
	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected Asset Panda LLC's customer support site or email alias and public change log or release notes to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
	The company provides a description of its products and services to internal and external users.	Inspected Asset Panda LLC's network diagram and product documentation to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected Asset Panda LLC's privacy policy and terms of service to determine that the company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
Risk Assessment			
CC 3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected Asset Panda LLC's completed risk assessment to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected Asset Panda LLC's Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
CC 3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected Asset Panda LLC's tabletop disaster recovery exercise to determine that the company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected Asset Panda LLC's completed risk assessment to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected Asset Panda LLC's Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected Asset Panda LLC's Third-Party Management Policy and vendor information to determine that the company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	No exceptions noted.
CC 3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected Asset Panda LLC's completed risk assessment to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected Asset Panda LLC's Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected Asset Panda LLC's Operations Security Policy and CI/CD system to determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected Asset Panda LLC's penetration test report and remediation to determine that the company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected Asset Panda LLC's completed risk assessment to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected Asset Panda LLC's Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
Monitoring Activities			
CC 4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected Asset Panda LLC's continuous security monitoring in Vanta to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected Asset Panda LLC's penetration test report and remediation to determine that the company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected Asset Panda LLC's Third-Party Management Policy and vendor information to determine that the company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
CC 4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected Asset Panda LLC's continuous security monitoring in Vanta to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected Asset Panda LLC's Third-Party Management Policy and vendor information to determine that the company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	No exceptions noted.
Control Activities			
CC 5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected Asset Panda LLC's information security policies and procedures to determine that they are documented and reviewed at least annually.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected Asset Panda LLC's Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected Asset Panda LLC's Secure Development Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected Asset Panda LLC's information security policies and procedures to determine that they are documented and reviewed at least annually.	No exceptions noted.
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected Asset Panda LLC's Access Control Policy to determine that the company's policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	No exceptions noted.
CC 5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected Asset Panda LLC's Data Management Policy to determine that the company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected Asset Panda LLC's changes to software and infrastructure components to determine that they were authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected Asset Panda LLC's Secure Development Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company's data backup policy documents requirements for the backup and recovery of customer data.	Inspected Asset Panda LLC's Data Management and Operations Security Policy to determine that the company's data backup policy documents requirements for the backup and recovery of customer data.	No exceptions noted.
	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Asset Panda LLC's Information Security Roles and Responsibilities to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected Asset Panda LLC's information security policies and procedures to determine that they are documented and reviewed at least annually.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected Asset Panda LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected Asset Panda LLC's completed risk assessment to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected Asset Panda LLC's Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected Asset Panda LLC's Third-Party Management Policy and vendor information to determine that the company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	No exceptions noted.
Logical and Physical Access			
CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company maintains a formal inventory of production system assets.	Inspected Asset Panda LLC's inventory items to determine that the company maintains a formal inventory of production system assets.	No exceptions noted.
	The company restricts access to migrate changes to production to authorized personnel.	Inspected Asset Panda LLC's application changes and version control system to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.
	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as a unique SSH key.	Inspected Asset Panda LLC's authentication to production datastores to determine that they use authorized secure authentication mechanisms, such as a unique SSH key.	No exceptions noted.
	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected Asset Panda LLC's Cryptography Policy to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected Asset Panda LLC's user data encryption to determine that the company's datastores housing sensitive customer data are encrypted at rest.	No exceptions noted.
	The company requires authentication to systems and applications to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected Asset Panda LLC's authentication to systems and applications to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected Asset Panda LLC's Data Management Policy to determine that the company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
	System access is restricted to authorized access only.	Inspected Asset Panda LLC's access to the application to determine that the system access is restricted to authorized access only.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected Asset Panda LLC's Access Control Policy to determine that the company's policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	No exceptions noted.
	The company restricts privileged access to databases to authorized users with a business need.	Inspected Asset Panda LLC's MongoDB Atlas accounts to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected Asset Panda LLC's firewall configuration to determine that the company restricts privileged access to the firewall to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected Asset Panda LLC's MongoDB Atlas accounts to determine that the company restricts privileged access to the operating system to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the production network to authorized users with a business need.	Inspected Asset Panda LLC's access to the production network to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected Asset Panda LLC's access request ticket and history to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
	The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected Asset Panda LLC's SSL/TLS on the admin page of the infrastructure console to determine that the company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected Asset Panda LLC's password policy configuration to determine that the company requires passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected Asset Panda LLC's production systems to determine that they can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected Asset Panda LLC's SSL/TLS on the admin page of the infrastructure to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
	The company's network is segmented to prevent unauthorized access to customer data.	Inspected Asset Panda LLC's network segregation to determine that the company's network is segmented to prevent unauthorized access to customer data.	No exceptions noted.
CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected Asset Panda LLC's Access Control Policy to determine that the company's policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	No exceptions noted.
	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected Asset Panda LLC's completed access review to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected Asset Panda LLC's sample of completed access revocation to determine that the company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected Asset Panda LLC's access request ticket and history to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
	The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected Asset Panda LLC's SSL/TLS on the admin page of the infrastructure console to determine that the company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected Asset Panda LLC's Access Control Policy to determine that the company's policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	No exceptions noted.
	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected Asset Panda LLC's completed access review to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected Asset Panda LLC's sample of completed access revocation to determine that the company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected Asset Panda LLC's access request ticket and history to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
	The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected Asset Panda LLC's SSL/TLS on the admin page of the infrastructure console to determine that the company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The entity does not operate any physical hardware such as servers and network devices but rather uses subservice organizations and relies on its own controls for physical access.	Not Applicable - Control is implemented and maintained by subservice organizations.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
CC 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected Asset Panda LLC's Asset and Data Management Policy to determine that the company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no electronic media disposal occurred during the review period.
	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected Asset Panda LLC's Data Management Policy to determine that the company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.
	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected Asset Panda LLC's customer data deletion record to determine that the company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	No exceptions noted.
	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected Asset Panda LLC's sample of completed access revocation to determine that the company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	No exceptions noted.
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected Asset Panda LLC's SSL/TLS on the admin page of the infrastructure console to determine that the company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected Asset Panda LLC's production systems to determine that they can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected Asset Panda LLC's SSL/TLS on the admin page of the infrastructure to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected Asset Panda LLC's intrusion detection system to determine that it is configured to continuously monitor the company's network and early detection of potential security breaches.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected Asset Panda LLC's SSL/TLS settings on the company website to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected Asset Panda LLC's firewall rulesets to determine that they are reviewed at least annually. Required changes are tracked to completion.	No exceptions noted.
	The company uses firewalls and configures them to prevent unauthorized access.	Inspected Asset Panda LLC's firewall configuration to determine that the company uses firewalls and configures them to prevent unauthorized access.	No exceptions noted.
	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected Asset Panda LLC's Operations Security Policy to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable devices when used.	Inspected Asset Panda LLC's encryption to determine that the company encrypts portable when used.	No exceptions noted.
	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected Asset Panda LLC's mobile device management (MDM) system to determine that it is in place to centrally manage mobile devices supporting the service.	No exceptions noted.
	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected Asset Panda LLC's SSL/TLS settings on the company website to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected Asset Panda LLC's Secure Development Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected Asset Panda LLC's malware detection settings on computers to determine that the company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
System Operations			
CC 7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected Asset Panda LLC's Operations Security Policy and CI/CD system to determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	No exceptions noted.
	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected Asset Panda LLC's changes to software and infrastructure components to determine that they were authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
	The company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	Inspected Asset Panda LLC's Operations Security Policy to determine that the company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected Asset Panda LLC's completed risk assessment to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
CC 7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected Asset Panda LLC's penetration test report and remediation to determine that the company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected Asset Panda LLC's intrusion detection system to determine that it is configured to continuously monitor the company's network and early detection of potential security breaches.	No exceptions noted.
	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected Asset Panda LLC's log management tool to determine that the company utilizes a system to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected Asset Panda LLC's infrastructure monitoring tool to determine that it is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
	The company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	Inspected Asset Panda LLC's Operations Security Policy to determine that the company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
CC 7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected Asset Panda LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected Asset Panda LLC's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company tests its incident response plan at least annually.	Inspected Asset Panda LLC's incident response tabletop exercise to determine that the company tests its incident response plan at least annually.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected Asset Panda LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected Asset Panda LLC's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected Asset Panda LLC's tabletop disaster recovery exercise to determine that the company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	No exceptions noted.
	The company tests its incident response plan at least annually.	Inspected Asset Panda LLC's incident response tabletop exercise to determine that the company tests its incident response plan at least annually.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected Asset Panda LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected Asset Panda LLC's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
Change Management			
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected Asset Panda LLC's changes to software and infrastructure components to determine that they were authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
	The company restricts access to migrate changes to production to authorized personnel.	Inspected Asset Panda LLC's application changes and version control system to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected Asset Panda LLC's Secure Development Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected Asset Panda LLC's penetration test report and remediation to determine that the company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected Asset Panda LLC's Operations Security Policy to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected Asset Panda LLC's vulnerability scan and a sample of remediated vulnerabilities to determine that the host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of Asset Panda LLC's Controls</i>	<i>Service Auditor Test of Controls</i>	<i>Results of Service Auditor Test of Controls</i>
Risk Mitigation			
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected Asset Panda LLC's Business Continuity and Disaster Recovery Plan to determine that the company has a policy in place that outlines communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected Asset Panda LLC's cybersecurity insurance policy to determine that the company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected Asset Panda LLC's completed risk assessment to determine that the company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected Asset Panda LLC's Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected Asset Panda LLC's privacy policy and terms of service to determine that the company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected Asset Panda LLC's Third-Party Management Policy and vendor information to determine that the company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	No exceptions noted.

CERTIFICATE *of* SIGNATURE

REF. NUMBER
UJBSI-TTUTM-EDSSI-I2V23

DOCUMENT COMPLETED BY ALL PARTIES ON
28 MAY 2025 15:39:54 UTC

SIGNER

JONATHAN LARKIN

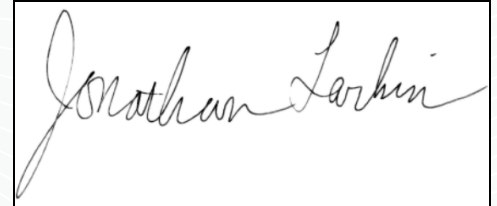
EMAIL
JONATHAN@ASSETPANDA.COM

TIMESTAMP

SENT
28 MAY 2025 15:39:54 UTC

SIGNED
28 MAY 2025 15:39:54 UTC

SIGNATURE



IP ADDRESS
107.128.58.36

LOCATION
FRISCO, UNITED STATES






AssetPanda_OntarioSenecaBOCES_NY_11State_OHG_VendorSigned

Final Audit Report

2025-05-29

Created:	2025-05-29
By:	Michael Klisiwecz (mklisiwecz@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAjWYrnGOI_gbq-jH8mXdeQyYFDPfsiww

"AssetPanda_OntarioSenecaBOCES_NY_11State_OHG_VendorSigned" History

-  Document created by Michael Klisiwecz (mklisiwecz@tec-coop.org)
2025-05-29 - 5:39:06 PM GMT
-  Document emailed to Kelli Eckdahl (kelli.eckdahl@edutech.org) for signature
2025-05-29 - 5:39:18 PM GMT
-  Email viewed by Kelli Eckdahl (kelli.eckdahl@edutech.org)
2025-05-29 - 8:12:04 PM GMT
-  Document e-signed by Kelli Eckdahl (kelli.eckdahl@edutech.org)
Signature Date: 2025-05-29 - 8:13:26 PM GMT - Time Source: server
-  Agreement completed.
2025-05-29 - 8:13:26 PM GMT