

**MASSACHUSETTS STUDENT DATA PRIVACY AGREEMENT
VERSION (2018)**

Dedham Public Schools

and

Pixel Press Technology LLC

August 3, 2018

This Massachusetts Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Dedham Public Schools (hereinafter referred to as "LEA") and Pixel Press Technology LLC (hereinafter referred to as "Provider") on August 03, 2018. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") as described in Article I and Exhibit "A"; and

WHEREAS, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in Massachusetts the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq.; and

WHEREAS, the documents and data transferred from Massachusetts LEAs and created by the Provider's Services are also subject to several Massachusetts student privacy laws, including Massachusetts student record regulations, 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 this 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.

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

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 (as defined in Exhibit "C") transmitted to Provider from the LEA pursuant to Exhibit "A", including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") are transmitted to Provider from LEA, 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. Control duties are set forth below.
2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described in Exhibit "A".

3. **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit "A", LEA shall provide the categories of data described in the Schedule of Data, attached hereto as Exhibit "B".
4. **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 all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. The Provider will cooperate and provide Student Data within ten (10) days at the LEA's request. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall cooperate and respond within ten (10) days to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of 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.** Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.
4. **Third Party Request.** Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a

compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. 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.

5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws.** LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H, and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected 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 Massachusetts and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, , 603 C.M.R. 23.00 and Massachusetts General Law, Chapter 71, Sections 34D to 34H.
2. **Authorized Use.** Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, any student data, meta data, user content or other non-public

information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.
4. **No Disclosure.** De-identified information, as defined in Exhibit "C", may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). The Provider and LEA agree that the Provider cannot successfully de-identify information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, *i.e.*, twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. Provider agrees not to attempt to re-identify de-identified Student Data and 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. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA.
5. **Disposition of Data.** Provider shall dispose or delete all personally identifiable data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" FORM, A Copy of which is attached hereto as Exhibit "D"). Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within three (3) calendar days of receipt of said request.
6. **Advertising Prohibition.** Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or advertising efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client; or (d) use the

Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.
 - b. **Destruction of Data.** Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.
 - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.
 - d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
 - e. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.
 - f. **Security Coordinator.** Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the DPA.
 - g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the

terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
- i. Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.
- j. Audits.** Upon receipt of a request from the LEA, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof. The Provider will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide full 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 Provider. Failure to cooperate shall be deemed a material breach of the Agreement.

2. Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within ten (10) days of the incident. Provider shall follow the following process:

- a.** The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
- b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

 - 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.
 - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

- c. At LEA's discretion, the security breach notification may also include any of the following:
 - i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. Provider agrees to adhere to all requirements in the Massachusetts Data Breach law and in federal law 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.
- e. 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 copy of said written incident response plan.
- f. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.
2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any terms of this DPA.

3. **Effect of Termination Survival.** If the DPA is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).
4. **Priority of Agreements.** This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA, IDEA, COPPA, PFRA, 603 CMR 28.00, 603 C.M.R. 23.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.

5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives below.

The designated representative for the Provider for this Agreement is:

Name	<u>DORIN LATH</u>
Title	<u>CEO</u>
Address	<u>317 N. 11TH ST. SUITE 500 ST. LOUIS MO 63101</u>
Telephone Number	<u>314-814-2357</u>
Email	<u>DORIN@PROJECTPIXELPRESS.COM</u>

The designated representative for the LEA for this Agreement is:

Title	Technology Director
Address	100 Whiting Avenue, Dedham, MA 02026
Telephone Number	(781) 310-1000

6. **Entire Agreement.** This DPA constitutes 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.

7. **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.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND

CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF MASSACHUSETTS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF [COUNTY OF LEA] COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.
10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Electronic Signature:** The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with Massachusetts and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of my electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

If either party would like a paper copy of this Agreement, they may request a copy from the other party.

12. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

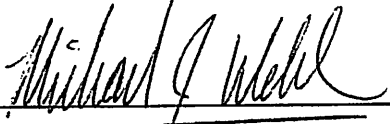
ARTICLE VII- GENERAL OFFER OF TERMS

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 this to any other school district who signs the acceptance in said Exhibit.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Massachusetts Student Data Privacy Agreement as of the last day noted below.

DEDHAM PUBLIC SCHOOLS

 Date: 9-11-2018
Printed Name: Michael J. Welch Title: Superintendent

PIXEL PRESS TECHNOLOGY LLC


 Date: 9/6/2018
Printed Name: Brian Rath Title: CEO

EXHIBIT "A"
DESCRIPTION OF SERVICES

<http://edu.bloxelsbuilder.com/>

Online video game development application.

•

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.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	✓
Assessment	Standardized test scores	
	Observation data	✓
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	✓
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred 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	
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	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
Category of Data	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/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	

Category of Data	Elements	Check if used by your system
	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	

EXHIBIT “C”

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de-identified if there are fewer than twenty (20) students in the samples of a particular field or category, i.e., twenty students in a particular grade or less than twenty students with a particular disability.

NIST 800-63-3: Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes, without limitation, at least the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student’s Educational Record

Information in the Student’s Email

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 pupil records.

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education 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 pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

School Official: For the purposes of this Agreement 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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records. The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02.

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, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Massachusetts and Federal 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.

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

Subprocessor: For the purposes of this Agreement, 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 software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

Third Party: The term “Third Party” means an entity that is not the provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] directs [Name of Company] to dispose of data obtained by Company pursuant to the terms of the DPA 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] STUDENT FIRST + LAST NAME, STUDENT CREATED

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

CONTENT IN
SYSTEM

2. Nature of Disposition

X 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. Timing of Disposition

Data shall be disposed of by the following date:

X 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

9/6/2018
Date

OPTIONAL: EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? ☒ Yes ☐ No

If yes, please provide it. ATTACHED

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

☐ ISO 27001/27002

☐ CIS Critical Security Controls

☐ NIST Framework for Improving Critical Infrastructure Security

☐ Other: _____

3. Does your organization store any customer data outside the United States? ☐ Yes ☒ No
4. Does your organization encrypt customer data both in transit and at rest? ☐ Yes ☐ No
5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: BOB BENNET

Contact information: BOB@PROJECTPIXELPRESS.COM

6. Please provide any additional information that you desire.

Pixel Press Technology LLC
Information and Data Security Policy
v1.0 September 6, 2018

Security Policy #1

Written Information Security Policy (WISP)

Statement of Policy

The objective of Pixel Press ("The Company") in the development and implementation of this comprehensive written information security policy ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personally identifiable information (PII) of customers, clients and employees as well as sensitive company information that could harmful if unauthorized access were to occur. The WISP sets forth a procedure for evaluating and addressing electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII and sensitive company information.

*The use of the term **employees** will include all of The Company's owners, managers, employees, all independent contractors and temporary employees.*

Purpose of Policy

The purpose of the WISP is to better:

- 1) Ensure the security and confidentiality of **personally identifiable information (PII)** of customers, clients, employees or vendors as well as **sensitive company data** which includes emails, confidential company information (i.e. company expansion plans, manufacturing processes, highly secretive information, etc.), employee information and the like.;
- 2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and
- 3) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft, fraud or harm to The Company.

Scope of Policy

In formulating and implementing the WISP, The Company has addressed and incorporated the following protocols:

- 1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII and sensitive company data.
- 2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII and sensitive company data.
- 3) Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risk.
- 4) Designed and implemented a WISP that puts safeguards in place to minimize identified risks.
- 5) Implemented regular monitoring of the effectiveness of those safeguards.

Security Safeguards

The follow safeguards are effective immediately. The goal of implementing these safeguards are to protect against risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII or sensitive company data.

Administrative Safeguards

- 1) **Security Officer** - The Company has designated [INSERT EMPLOYEE NAME] to implement, supervise and maintain the WISP. This designated employee (the "Security Officer") will be responsible for the following:
 - (a) Implementation of the WISP including all provisions outlined in **Security Safeguards**.
 - (b) Training of all employees that may have access to PII and sensitive company data. Employees should receive annual training and new employees should be trained as part of the new employee hire process.
 - (c) Regular monitoring of the WISP's safeguards and ensuring that employees are complying with the appropriate safeguards.
 - (d) Evaluating the ability of any Third Party Service Providers to implement and maintain appropriate security measures for the PII and sensitive company data to which The Company has permitted access, and requiring Third Party Service Providers, by contract, to implement and maintain appropriate security measures.
 - (e) Reviewing all security measures at least annually, or whenever there is a material change in The Company's business practices that may put PII and sensitive company data at risk.
 - (f) Investigating, reviewing and responding to all security incidents or suspected security incidents.
- 2) **Security Management** - All security measures will be reviewed at least annually, or whenever there is a material change in The Company's business practices that may put PII or sensitive company data at risk. This should include performing a security risk assessment, documenting the results and implementing the recommendations of the security risk assessment to better protect PII and sensitive company data. The Security Officer will be responsible for this review and will communicate to management the results of that review and any recommendations for improved security arising out of that review.

- 3) **Minimal Data Collection** - The Company will only collect PII of clients, customers or employees that is necessary to accomplish legitimate business transactions or to comply with any and all federal, state or local regulations.
- 4) **Information Access** - Access to records containing PII and/or sensitive company data shall be limited to those persons whose job functions requires a legitimate need to access the records. Access to the records will only be for a legitimate job-related purpose. In addition, pre-employment screening should take place to protect PII and sensitive company data.
- 5) **Employee Termination** - Terminated employees must return all records containing PII and sensitive company data, in any form, that may be in the former employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.). A terminated employee's physical and electronic access to PII and sensitive company data must be immediately blocked. A terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to The Company's premises or information. A terminated employee's remote electronic access to PII and sensitive company data must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated. See **Security Policy #2 – Termination Policy**.
- 6) **Security Training** – All employees, which includes all owners, managers, employees, all independent contractors and temporary employees that may have access to PII and sensitive company data, will receive security training . Employees should receive at least annual training and new employees should be trained as part of the new employee hire process. Employees should be required to show their knowledge of the information and be required to pass an exam that demonstrates their knowledge. Documentation of employee training should be kept and reviewed.
- 7) **WISP Distribution** - A copy of the WISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing or electronically, that he/she has received a copy of the WISP and will abide by its provisions. See **Security Policy #1 - Written Information Security Policy (WISP) Appendix A – WISP Employee Acknowledgement Form**.
- 8) **Contingency Planning** – All systems that store PII and/or sensitive company data should have the data backed up on, at least, a nightly basis. Data should be encrypted and be stored offsite. Disaster Recovery mechanisms and documented procedures should be in place to restore access to PII and sensitive company data as well as any operational systems that The Company relies on. A system criticality assessment should be performed that defines how critical each of The Company's systems are. Systems that are critical to operations should be restored before non-critical systems. On a periodic basic, data

backups, data restoration and Disaster Recovery procedures should be tested and validated. See Disaster Recovery Template.

- 9) **Security Incident Procedures** - Employees are required to report suspicious or unauthorized use of PII and/or sensitive company data to a supervisor or the Security Officer. Whenever there is an incident that requires notification pursuant to any federal or state regulations, the Security Officer will conduct a mandatory post-incident review of the events and actions taken in order to determine how to alter security practices to better safeguard PII and sensitive data. See Security Policy #3- Security Incident Response.
- 10) **Emergency Operations** – Procedures should be in place to define how The Company will respond to emergencies. Procedures should include employee contact information, critical vendor contact information, important vendor account information as well as any emergency operating procedures. See Emergency Operations Template.
- 11) **Data Sensitivity Classification** – All data that The Company stores or accesses should be categorized in terms of the sensitive nature of the information. For example, PII and sensitive company data might have a very high sensitivity and should be highly protected. Whereas publicly accessible information might have a low sensitivity and requires minimal protection.
- 12) **Third Party Service Providers** - Any service provider or individual (“Third Party Service Provider”) that receives, stores, maintains, processes, or otherwise is permitted access to any file containing PII and/or sensitive company data shall be required to protect PII and sensitive company data. The Third Party Service Providers must sign service agreements that contractually hold them responsible for protecting The Company’s data. Examples include third parties who provide off-site backup of electronic data; website hosting companies; credit card processing companies; paper record copying or storage providers; IT / Technology Support vendors; contractors or vendors working with customers and having authorized access to PII and/or sensitive company data.
- 13) **Sanctions** - All employment contracts, where applicable, should be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of PII and/or sensitive company data as defined by the WISP. Disciplinary actions will be taken for violations of security provisions of the WISP (The nature of the disciplinary measures may depend on a number of factors including the nature of the violation and the nature of the PII and/or sensitive company data affected by the violation). See Security Policy #4 – Sanction Policy.
- 14) **Bring Your Own Device (BYOD) Policy** – The Company may allow employees to utilize personally owned devices such as laptops, smartphones and tablets. If allowed, proper safeguards must be implemented to protect PII and sensitive company data that may be

accessed or stored on these devices. Employees must understand what are the requirements for using personally owned devices and what safeguards are required. See **Security Policy #9 – BYOD Policy**.

Physical Safeguards

- 15) **Facility Access Controls** – The Company will implement physical safeguards to protect PII and sensitive company data. There will be physical security on facilities / office buildings to prevent unauthorized access. All systems that access or store PII and/or sensitive company data will be physically locked. Employees will be required to maintain a “clean desk” and ensure that PII and/or sensitive company data is properly secured when they are not at their desk. The Security Officer will maintain a list of lock combinations, passcodes, keys, etc. and which employees that have access to the facilities and PII and/or sensitive data. Visitors will be restricted from areas that contain PII and/or sensitive company data. See **Security Policy #10 - Facility Security Plan**.
- 16) **Network Security** – The Company will implement security safeguards to protect PII and sensitive company data. Safeguards include; isolating systems that access or store PII and/or sensitive company data, the use of encryption on all portable devices, physical protection on portable devices, ensuring that all systems run up-to-date anti-malware, implementing network firewalls, performing periodic vulnerability scans, capturing and retaining network log files as well as ensuring that servers and critical network equipment are stored in an environmentally safe location. See **Security Policy #5 – Network Security**

Technical Safeguards

- 17) **Access Control** - Access to PII and sensitive company data shall be restricted to approved active users and active user accounts only. Employees will be assigned unique user accounts and passwords. Systems containing PII and sensitive company data should have automatic logoff procedures to prevent unauthorized access. **See Security Policy #6 – Access Control**
- 18) **Computer Use** – All employees will be given a Computer Use Policy that defines acceptable and unacceptable use of The Company’s computing resources. Employees should be required to sign the Computer Use Policy to acknowledge acceptance of the policy. **See Security Policy #7 – Computer Use**
- 19) **Data Disposal** - Written and electronic records containing PII and sensitive company data shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements. **See Security Policy #8 – Equipment Disposal**
- 20) **System Activity Review** - All systems that store or access PII and sensitive company data should utilize a mechanism to log and store system activity. Periodic system activity reviews should occur and identify unauthorized access to PII and sensitive company data. Any unauthorized access should be reported to the Data Security Coordinator. **See Security Policy #3- Security Incident Response**
- 21) **Encryption** - To the extent technically feasible all portable devices that contain PII and sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII and sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

Appendix A – WISP Employee Acknowledgement Form

I have read, understand, and agree to comply with the Written Information Security Policy (WISP), rules, and conditions governing the security of PII and sensitive company data. I am aware that violations of the WISP may subject me to disciplinary action and may include termination of my employment.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

Signature

Date

Employee's Supervisor Signature

Date

Security Policy #3

Security Incident Procedures

Purpose of Policy

The purpose of the policy is to develop the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

It should be noted that breach definitions, remediation steps and breach notification steps vary between various federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), The Gramm-Leach-Bliley Act (GLB Act or GLBA) and other federal regulations. In addition, most state regulated breach laws vary between individual states. It is highly recommended to consult with breach experts or legal counsel to determine The Company's responsibilities.

Definitions

Breach

Breach means the acquisition, access, use, or disclosure of personally identifiable information (PII) or sensitive company data such as email, employee information, confidential information, etc. which compromises the security or privacy of the PII or sensitive company data.

Unsecured PII

Unsecured PII means PII that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology such as encryption. The definition of unsecured PII varies between different federal and state regulations.

Reporting and Response

1. The Company will ensure that all incidents, threats, or violations that affect or may affect the privacy, confidentiality, integrity, or availability of PII and sensitive company data will be reported and responded to.

2. The Company shall have a Security Incident Response Team (SIRT) charged with the responsibility of identifying, evaluating and responding to security incidents. The Privacy Security Officer shall oversee the activities of the SIRT.
 - a. The SIRT will be responsible for investigating all known or suspected privacy and security incidents.
 - b. The SIRT will document a procedure for all employees to follow to report privacy and security incidents. See **Appendix A – Security Incident Response Log or the Security Incidents Module in the Security Portal.**
 - c. The Company will ensure that all employees receive training on how to identify and report security incidents.
 - d. All employees must follow the documented procedure to report security incidents. In addition, employees must report all known or suspected security incidents.
 - e. All employees must assist the SIRT with any security incident investigations.

Breach Determination

The Security Incident Response Team (SIRT) will investigate all reported and suspected security breaches. The SIRT will refer to federal or state regulations to help with breach determination. Breach determination varies between federal regulations such as HIPAA and GLBA. In addition, breach determination varies significantly between state regulations (for example, what may be considered a breach in one state may not be a breach in another state).

Breach Notification

If the SIRT determines that a breach of unsecured PII has occurred, breach notification of affected individuals may be required. The SIRT will refer to federal or state regulations to help with breach notification requirements. Breach notification requirements varies between federal regulations such as HIPAA and GLBA. In addition, breach notification requirements varies significantly between state regulations (for example, one state may have breach notification requirements that varies significantly from breach notification requirements in another state).

Key elements of a breach notification include:

I. Date of discovery

Usually a breach will be treated as discovered as of the first day the breach is known or by exercising reasonable diligence would have been known.

II. Timeliness of notification

The Company will provide the required notifications without unreasonable delay after discovery of a breach. The amount of time The Company has to notify affected individuals varies between federal and state regulations.

III. Content of notification

If required, a notification will be provided to each individual affected by the discovered breach. The notification should include the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PII that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what The Company is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which should include a telephone number, an e-mail address, Web site, or postal address.
- The notification should be written in plain language.

IV. Methods of notification

The following methods are usually used to notify individuals affected by the discovered breach:

i. Written notice

Written notification by first-class mail to the individual at the last known address of the individual or, via e-mail if the individual agrees to e-mail notice. The notification may be provided in one or more mailings as information is available.

If the individual is deceased notifications are usually sent to next of kin or personal representative

ii. Substitute notice

If contact information is out of date and written notification cannot be made, a substitute notification may be used.

- A substitute notification usually in the form of either a conspicuous posting on The Company's home page of its Web site, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The notice should include a contact phone number.

V. Notification to media

In addition to notifying individuals of a known breach, a notification to the media may be required as well.

VI. Notification to federal or state regulatory agencies

The Company may need to report breaches of unsecured information to federal or state regulatory agencies.

VII. Notification by Third Party Service Providers

Third Party Service Provider responsible for a breach of The Company's PII or sensitive company data should be required to notify The Company within a pre-determined reasonable timeframe. The timeframe should be defined in a Service Provider Agreement.

Third Party Service Provider breaches may result in The Company having to notify The Company's affected individuals (such as customers, employees, etc.).

Appendix A – Security Incident Response Log

Incident Identification Information	
Name:	
Phone:	
Email:	
Date/Time Detected:	
System / Application Affected:	
Incident Summary	
Type of Incident Detected: (Denial of Service, Malicious Code, Unauthorized Access, Unauthorized Use / Disclosure, Unplanned System Downtime, Other)	
Description of Incident:	
Names of Others Involved:	
Incident Notification	
How Was This Notified? (Security Office, IT Personnel, Human Resources, Other)	
Response Actions Include Start and Stop times	
Identification Measures (Incident Verified, Accessed, Options Evaluated):	
Containment Measures:	
Evidence Collected (Systems Logs, etc.):	

Security Policy #4

Sanction Policy

Scope of Policy

This policy governs employee Sanctions and disciplinary actions for The Company. All employees must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every employee.

Policy Statement

- It is the Policy of The Company to establish and implement appropriate, fair and consistent sanctions for employees who fail to follow established policies and procedures, or who commit various offenses.
- Sanctions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
- Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.
- All employee Sanctions will be documented

Based on the severity of the violation, develop varying levels of disciplinary action such as:

- Verbal warning
- Written warning
- Education – training/retraining
- Removal of system privileges
- Suspension without pay
- Termination of employment

Procedures

- Inadvertent release of PII and sensitive company data will be investigated and the punishment will be determined by management and the extent of harm to individual involved.
- Employees accessing PII and sensitive company data files that they do not have a reason to access is a violation that may result in immediate termination.
- Blatant disregard for The Company's Policies and Procedures may result in immediate termination.
- Intentional release of PII and sensitive company data to someone who should not have access to the information WILL result in immediate termination and possible prosecution.

Optional Signature Line

Name [Print]: _____

Signature: _____

Security Policy #5

Network Security

Purpose of Policy

The purpose of the policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store PII and sensitive company data to ensure that appropriate security is maintained and that access is restricted to authorized employees.

Network Security

The Company will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers and portable devices including laptops, smartphones, CD-ROMs, DVDs, USB Drives, etc. that store or access PII and sensitive company data.

- 1) Workstations and laptops that are in common areas that store or access PII and/or sensitive company data should be physically placed with the monitor so that it prohibits unauthorized people from viewing confidential information such as logins, passwords, PII and/or sensitive company data.
- 2) Workstations and laptops that are in common areas that store or access PII and sensitive company data should utilize privacy screens to prevent unauthorized access to the data.
- 3) Workstations and laptops that are in common areas that store or access PII and sensitive company data should be secured by restraints such as locking cables.
- 4) To the extent technically feasible all portable devices that contain PII and/or sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII and/or sensitive company data across public networks and wireless networks. Public networks include email and Internet access.
- 5) Portable devices and media should be concealed from view when offsite to prevent theft.
- 6) All network servers, application servers, routers, database systems, device management system hardware, and other servers should be located in a room or an area that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel.
- 7) All workstations, servers and portable devices will run anti-virus / anti-malware software that protect against malicious software. The software must be current and up to date with virus / malware definitions. Employees must use and keep active current versions of approved anti-virus / anti-malware software scanning tools to detect and remove malicious

software from workstations and files. Employees must not disable these tools unless specifically directed by computer support personnel to do so in order to resolve a particular problem.

- 8) A network firewall should be in place to protect PII and/or sensitive company data. The firewall protection should be up to date. Firewalls should be monitored and alerts should be triggered in the event of unauthorized intrusion or suspected intrusion.
- 9) Log files from network equipment should be stored and retained. Log files from network equipment include; firewalls, network servers, desktops, laptops and other devices. The required length of retention of log files may vary depending on federal, state or industry regulations.
- 10) All workstations, servers and portable devices, where feasible, must implement a security patch and update procedure to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
- 11) Periodic network vulnerability scans should be performed on all internal as well as external (Internet facing servers, websites, etc.) systems. Results of the vulnerability scans should be analyzed and known vulnerabilities should be remediated and/or patched. After all vulnerabilities are remediated, an external network penetration test should be performed to ensure that unauthorized external access into the network is prevented.
- 12) Reasonable and appropriate steps will be taken to prevent unauthorized access to workstations, servers and portable devices from misuse and physical damage, vandalism, power surges, electrostatic discharge, magnetic fields, water, overheating and other physical threats.
 - a. Workstations must not be located where they will be directly affected by extremes of temperature or electromagnetic interference. Precautions should also be taken to ensure that workstations cannot be affected by problems caused by utilities, such as water, sewer and/or steam lines that pass through the facility.
 - b. All facilities that store systems that contain PII and/or sensitive company data, should have appropriate smoke and/or fire detection devices, sprinklers or other approved fire suppression systems, and working fire extinguishers in easily accessible locations throughout the facility.
 - c. All servers that contain PII and/or sensitive company data, should be connected to an Uninterrupted Power Supply (UPS) to prevent server crashes during power outages or spikes. Servers should be configured to shut down in a controlled manner if the power outage is for an extended period of time.
 - d. All systems should be connected to surge protectors, where feasible, to protect against power spikes and surges.

- 13) A user identification and password authentication mechanism shall be implemented to control user access to the system. (See Security Policy #6 - Access Control).
- 14) Employees who suspect any inappropriate or unauthorized use of workstations should immediately report such incident or misuse to the Security Officer.

Security Policy #6

Access Control

Purpose of Policy

The purpose of the policy is to assure that systems containing PII and/or sensitive company data are accessed only by those persons or software programs that have been granted appropriate access rights

Unique User Identification

- 1) Employees will be assigned a unique user identification (i.e. userid) in order to access any system or application that transmits, receives or stores PII and/or sensitive company data.
- 2) Each employee must ensure that their assigned user identification is appropriately protected and only used for legitimate access to systems or applications.
- 3) If an employee believes their user identification has been comprised, they must report the security incident.
- 4) Employees should be aware of the following password procedures to create and use strong passwords to protect PII and sensitive company data:
 - a. Should be a minimum of eight characters in length.
 - b. Should incorporate both upper and lower case letters (e.g. a-z and A-Z)
 - c. Should incorporate digits and punctuation characters as well as letters e.g., 0-9, (! @ # \$ % ^ & * () _ - + = { } [] ; ' ' | \ / ? < > , . ~ `)
 - d. Should not be words found in a Dictionary.
 - e. Should not include easily guessed information such as personal information, names, pets, birth dates, etc.
- 5) Employees should be aware of the following procedures to protect passwords:
 - a. Passwords should not be written down
 - b. Passwords should not be shared with other employees

- c. If an employee suspects that their password has been compromised they should report the incident immediately
- 6) Passwords should be changed at least every 90 days
- 7) After a number of failed password attempts, the employee's account should be disabled (e.g. 3 or 5 failed attempts)

Automatic Logoff

- 1) Systems that access or store PII and/or sensitive company data should implement an automatic logoff after a determined period of inactivity (i.e. 10 minutes of inactivity). Employees would need to login again to regain access and continue the session.
- 2) When leaving a server, workstation, or other computer system unattended, employees must lock or activate the system's automatic logoff mechanism (e.g. CTRL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing or accessing PII and/or sensitive company data.

Encryption and Decryption

- 1) To the extent technically feasible all portable devices that contain PII and/or sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII or sensitive company data across public networks and wireless networks. Public networks include email and Internet access.
- 2) Employees should be trained on the use of encryption to protect PII and sensitive company data.
- 3) All backup tapes and media that contain PII and/or sensitive company data should utilize encryption to protect the data.
- 4) Secure encrypted remote access procedures should be implemented to protect systems that access or store PII and/or sensitive company data.
 - a. Authentication and encryption mechanisms should be required for all remote access sessions to networks containing PII and/or sensitive company data. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and encrypted Citrix/RDP client access.
 - b. Two-factor authentication (i.e. SMS pin notification) should be implemented where technically feasible.

5) All wireless access to networks should utilize encryption mechanisms.

a. Employees should not utilize open public Wi-Fi networks

Security Policy #7

Computer Use

Purpose of Policy

The purpose of this policy is to ensure that employees understand what functions should and should not be performed on The Company's computers and network to maximize the security of PII and sensitive company data. The policy also provides guidance regarding proper safeguards of PII and sensitive company data when accessing social media sites.

Computer Use

- 1) To ensure that workstations and other computer systems that may be used to send, receive, store or access PII and sensitive company data are only used in a secure and legitimate manner, all employees must comply with The Company's Computer Use Policy, a copy of which is attached as Appendix A.
- 2) The Company may provide workstations and other computer systems to employees for the purpose of performing their job functions. Employees shall be responsible for using workstations appropriately in conformance with this Policy.
- 3) The Company may remove or deactivate any employee's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.
- 4) Employees must be assigned and use a unique User Identification and Password (See **Security Policy #6 - Access Control**)
- 5) Employees that use The Company's information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, The Company may log, review, or monitor any data stored or transmitted on its information system assets.

Appendix A

Computer Use Policy

Introduction

This document provides guidelines for appropriate use of computer facilities and services. It is not a comprehensive document covering all aspects of computer use. It offers principles to help guide employees, and specific policy statements serve as a reference point. It will be modified as new questions and situations arise.

Computers, the Internet and electronic mail (e-mail) are powerful research, communication, commerce and time-saving tools that are made available to employees. The use of this efficient and effective communication tool is critical but, like any tools, computers, the Internet and e-mail have the potential to be used for inappropriate purposes.

Workstations and other computer systems may be provided to employees for the purpose of performing their job functions. Employees shall be responsible for using workstations appropriately in conformance with this Policy.

Policy

The following policies on computer, the Internet and electronic mail usage shall be observed by all employees.

- Users of the Internet and e-mail are to comply with all appropriate laws, regulations and generally accepted Internet etiquette.
- Primary purpose of the Internet and e-mail is to conduct official business.
- Users should identify themselves properly when using the Internet and e-mail, conduct themselves professionally, and be aware that their activities reflect on the reputation and integrity of all our employees.
- Each user is individually responsible for the content of any communication sent over or placed on the Internet and e-mail.
- All employees have a responsibility to ensure a respectful workplace. Computer equipment must not be used to visit Internet sites that contain pornographic or sexually explicit information, pictures, or cartoons.
- Exceptions to this policy are only allowed when pre-approved by supervisors or company management and deemed necessary for official business, research or investigatory work.

The following actions are prohibited. It is unacceptable for employees to:

- Knowingly or intentionally publish, display, transmit, retrieve or store inappropriate or offensive material on any department computer system.
- Create or distribute defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material.
- View or distribute obscene, pornographic, profane, or sexually oriented material.
- Violate laws, rules, and regulations prohibiting sexual harassment.
- Engage in any unauthorized activities for personal financial gain.
- Place advertisements for commercial enterprises, including but not limited to, goods, services or property.
- Download, disseminate, store or print materials including articles and software, in violation of copyright laws.
- Download any software, including but not limited to games, screen savers, toolbars or any other browsing tools without the permission of supervisors, company management or IT staff.
- Violate or infringe on the rights of others.
- Conduct business unauthorized by the company.
- Restrict or inhibit other users from using the system or the efficiency of the computer systems.
- Cause congestion or disruption of networks or systems, including distribution of chain letters.
- Transmit incendiary statements, which might incite violence or describe or promote the use of weapons.
- Use the system for any illegal purpose or contrary to company policy or business interests.
- Connect a personal computer to the company network without having the computer checked by IT staff to insure no threatening viruses / programs infect the company network.
- Monitor or intercept the files or electronic communications of other employees or third parties.
- Hack or obtain access to systems or accounts they are not authorized to use.
- To disclose a Login ID(s) or password to anyone nor allow anyone to access any information system with someone else's Login ID(s) or passwords
- Use other people's Login ID(s) or passwords to access any information system for any reason.

- To post any PII or sensitive company data on social network sites, public forums, etc. This includes posting pictures of PII or sensitive company data or pictures of customers without permission.
- Employees shall not remove electronic media that contains PII or confidential or proprietary information unless such removal is authorized by an employee's supervisor or company management.

Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

Employees will immediately report any activity that violates this agreement to the employee's supervisor, company management or company Security Officer.

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of the company computer and telecommunications equipment and services. I understand that I have no expectation of privacy when I use any of the telecommunication equipment or services. I am aware that Internet and e-mail may be subject to monitoring. I am aware that violations of this guideline on appropriate use of the e-mail and Internet systems may subject me to disciplinary action, including termination from employment, legal action and criminal liability. I further understand that my use of the e-mail and Internet may reflect on the image of the company to our customers, competitors and suppliers and that I have responsibility to maintain a positive representation of company. Furthermore, I understand that this policy can be amended at any time.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it. The company may deny access to information systems if this Agreement is not returned signed and dated.

Signature

Date

Requestor's Immediate Supervisor Signature

Date

Access Agreement Approved by (printed name)

Date

Security Policy #8

Disposal Procedure

Purpose of Policy

All media containing PII and sensitive company data, will be disposed of in a manner that destroys the data and does not allow unauthorized access to the data.

Procedures for computer/hardware disposal

- 1) The Security Officer or delegate will notify the Information Technology (IT) department/company/individual of equipment that needs to be disposed of.
- 2) The Security Officer or delegate will determine data sensitivity of data to be disposed of. (See Data Classification Table below)
- 3) IT will assess the condition of the equipment, and:
 - a. IT will track the disposal of the device (type of hardware, serial number, etc). See Appendix A: Media Disposal Log
 - b. IT will run approved wiping software on all devices to make sure all PII and sensitive company data is removed from the device.
 - i. This may include physical destruction (See Methods of Destruction below)
 - c. IT will verify the hardware's data has been removed.
 - d. IT will dispose of the hardware.
- 4) The Security Officer or delegate / IT will document the destruction of the asset and keep a record. See Appendix A: Media Disposal Log.
- 5) If taken to outside facility - The media shall be taken to an approved, certified facility for erasure or destruction. A letter of certification regarding date and time of erasure/destruction shall be obtained.

Data Classification Table:

- 1) **Low (Unclassified)** - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
 - Basic operating system, personal files, etc.
- 2) **Med (Sensitive but not Confidential)** - Erase the data using any means such as reformatting or degaussing.
 - This would be for business related information which is not considered sensitive company data.
- 3) **High (Confidential)** - The data must be erased using an approved technology to make sure it is not readable using special technology techniques. (See method of destruction below)
 - This would be for PII and sensitive company data.

Examples of hardware devices include:

- Workstation
- Laptop
- Tablet (iPad/Android)
- Smartphones
- Server hard drives
- Memory stick (USB drives)
- CD ROM disk / DVD ROM
- Storage / Backup tape(s)
- Hard drives
- Copiers / Scanners / Fax machines
- Any equipment that contains PII or sensitive company data

Methods of Destruction Table:

Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable.)
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.
Destroy	<p>There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack.</p> <ul style="list-style-type: none"> • Disintegration, Pulverization, Melting, and Incineration. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • Shredding. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. <p>Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm).</p>

Appendix A - Media Disposal Log

The below data was disposed / destroyed as required in **Security Policy #8 – Equipment Disposal**

Date of Destruction: 1/15/2014

Authorized By: Click here to enter text.

Description of Information Disposed of or Destroyed (include Manufacturer/Model/Serial Number/etc):

Click here to enter text.

Backup of Personally Identifiable Information (PII) or sensitive company data? Required if PII or data is the only copy.

☐ Yes

☐ No

If Yes, List Backup Location: Click here to enter text.

Method of Destruction:

☐ **Clear** (One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable.)

☐ **Purge** (Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.)

☐ **Destroy** (Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.)

Destruction Method Used:

[Click here to enter text.](#)

Final Disposition of Media:

☐ Disposed

☐ Reused Internally

☐ Reused Externally (sold / donated / etc.)

☐ Returned to Manufacturer / Leasing Company / Vendor / etc.

☐ Other: [Click here to enter text.](#)

Save this log and retain indefinitely. Upload to the Security Portal.

Security Policy #9

Bring Your Own Device (BYOD) Policy

Purpose of Policy

The purpose of the policy is to develop the appropriate safeguards to protect PII and sensitive company data on employee personally owned devices. Proper security controls are essential to protect any sensitive information that may be on these devices. Documented instructions and requirements should be provided to all employees that may be accessing or storing PII and sensitive company data on their personally owned devices and acknowledgement of acceptance should be documented and retained.

Bring Your Own Device (BYOD) Policy

- 1) The Company may be responsible for any breaches of PII and may suffer consequences of breached sensitive company data that resulted from unsecured employee personally owned devices.
- 2) Employees must be aware that breaches or inappropriate use of their devices that may put PII and/or sensitive company data at risk may negatively affect customers, The Company and the employee themselves. The Company has the right to revoke an employee's access to PII and/or sensitive company data or levy sanctions laid forth in The Company's sanction policy.
- 3) Encryption of devices usually offers a safe harbor under federal and state regulations and is the strongest protection against a data breach. Encryption should be used on all devices that access or store PII and/or sensitive company data.
- 4) Employees are not permitted to access PII and/or sensitive company data, on personally owned devices, unless authorized and approved. Only approved devices that are properly configured will be given access to PII and/or sensitive company data.
- 5) The Company will limit who has access to PII and/or sensitive company data on their personally owned devices. The Company will provide employees with only the limited amount of access to PII and/or sensitive company data to perform their job function.
- 6) The organization and their Information Technology (IT) group/provider will work together to manage and enforce this Bring Your Own Device (BYOD) policy.

Procedure

- 1) The Company will communicate this policy to their employees. Employees must request permission to use personally owned devices and fill in the registration form provided.

- 2) The Company and IT will periodically review and update this policy when new requirements are implemented or when security requirements change. Employees must be notified of any changes and a document of their acceptance/acknowledgment should be collected.
- 3) The Company and IT reserve the right to monitor and inspect devices registered in its BYOD program to ensure that PII and sensitive company data are being properly protected.
- 4) Upon an employee's termination of employment, The Company and IT will ensure that any devices the employee has with PII and/or sensitive company data are returned to IT for a final analysis and removal of any PII and/or sensitive company data or applications that access PII and/or sensitive company data. This will be conducted as soon as possible to limit inappropriate access to PII and/or sensitive company data.
- 5) Documentation, acknowledgement and registration forms will be retained for all employees and kept in their employee folder. Documentation must also be provided to employees initially and upon request.

Appendix A

Bring Your Own Device Policy

This document provides the guidelines for a Bring Your Own Device (BYOD) policy for The Company. It offers principles to help guide employees and staff and can be modified by the company to better reflect their specific needs.

The Company's employees have the ability to bring and utilize various personal devices that may have the ability to access, store or transmit PII and/or sensitive company data. Devices include but are not limited to smartphones, tablets and laptops. Employees must be aware that when accessing PII and/or sensitive company data on their personally owned devices, they must protect that information. The ability for employees to utilize personally owned devices at the office should be treated as a privilege and The Company reserves the rights to revoke this privilege if an employee does not abide by the policies laid forth.

Devices Permitted

Smartphones accepted (brand and model): _____

Tablets accepted (brand and model): _____

Laptops: personally owned laptops must be accepted and approved by (company name) management.

Additional Devices: other additional personal devices that may access or store patient information must be approved by (company name) management and IT.

Specifically excluded devices: _____

Security Specifications

Mobile Device Management service:

Encryption service:

Anti-Malware/Anti-Virus service:

Minimum Operating System required (laptop):

Minimum Operating System required (smartphones):

Minimum Operating System required (tablets):

Secure texting application required:

System Inactivity timeout setting (minutes):

Email Encryption provider:

Security Requirements

- All devices must be password protected.
- Passwords must be complex; requiring a minimum of 6 characters, a combination of upper- and lower-case letters, numbers and symbols.
- Devices must lock after five incorrect password attempts.
- Devices must “time out” and require a password after a five minute period of inactivity.
- Text messages that may contain PII and/or sensitive company data must be sent through the secure texting application provided. **If a secure texting application has not been provided then employees should not send PII and/or sensitive company data via text.**
- Emails that are sent through the device containing PII and/or sensitive company data must be sent encrypted. **If secure email encryption is not provided, employees should not send email that contain PII and/or sensitive company data via email.**

Restrictions and Limitations

- “Rooted” or “Jailbroken” devices are not permitted to access PII and/or sensitive company data.
- Employees must notify management when selling, trading in, recycling or disposing of their personal devices.
- The employee’s device may have data remotely deleted / wiped if 1) the device is lost or stolen, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of The Company’s data and/or technology infrastructure.
- Devices that are lost or stolen must be reported to management and/or IT as soon as possible but within 24 hours.
- Employees must inform management and/or IT if they plan to upgrade, recycle or dispose of their personally owned device.
- Employees who voluntarily resign from the organization must present their device(s) to management and/or IT within 48 hours to have all PII and/or sensitive company data and/or access deleted / removed from the device.
 - Employees who do not turn over their device(s) to management and/or IT within 48 hours after voluntary resignation are subject to a full remote wipe / deletion of all data including non PII and sensitive company data on their device.
- The organization will prepare for scheduled terminations in advance and ensure that employees present their device(s) to management and/or IT the day of the scheduled termination to have all PII and sensitive company data and/or access deleted / removed from the device. Terminated employees that do not present their device(s) will be given an opportunity to bring in their device(s) to have all PII and sensitive company data removed from the device(s). Terminated employees that fail to bring in their device(s), after given the opportunity, are subject to a full remote wipe / deletion of all data including non PII and/or sensitive company data on their device.

Additional Information

The organization will provide any additional specifications, requirements or restrictions in this section.

Sanctions

Violations or abuse of this policy are subject to the repercussions laid out in The Company's sanction policy.

Bring Your Own Device – Device Registration form

Employee name: _____

Position/title: _____

Phone number: _____ Secondary Phone number: _____

Device and Description: _____

Serial Number: _____ MAC Address: _____

Access points; where will patient information be accessed (email, text messages, applications, web etc.):

Device Security Specifications (for IT and/or (company name) management to complete):

Security Specification	Implemented (yes or no)	Details or additional information
Operating system		
Encryption		
Anti-virus service		
Secure Texting Application		
Timeout/lock settings		
Password requirements		
Web browser		
Mobile wipe		
E-mail provider		

Additional information, specific device restrictions and requirements should be detailed below:

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of personally owned devices that may access, store or transmit PII and sensitive company data. I am aware that violations of this guideline of appropriate use may subject me to retraction of this privilege or disciplinary action, including termination of employment. I further understand that inappropriate use of my device that may put PII and sensitive company data at risk may negatively affect customers, The Company and myself.

I am aware of the technical restrictions and requirements on my device that were provided in the device registration form. I will maintain and manage these security requirements on my device for as long as I continue to access, store or transmit PII and sensitive company data. I understand that The Company reserves the right to protect their customer's information as well as sensitive company data that I may be accessing and therefore have the ability to remotely wipe / delete data from my device if the need arises.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

Signature

Date

Requestor's Immediate Supervisor Signature

Date

Information Technology Provider's Signature

Date

Security Policy #10

Facility Security Plan

Purpose of Policy

The purpose of the policy is to define the procedures that will limit physical access to PII and sensitive company data and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

Facility Security Plan

- 1) Physical security of office buildings must be implemented to protect PII and sensitive data as well as other company assets. Physical measures might include: alarm systems, surveillance camera, fences, locked gates / doors, etc.
- 2) All systems that store or access PII and/or sensitive company data should be stored in locked rooms, closets or cabinets to prevent unauthorized access. Access to these facilities should be minimized and limited to only employees and/or vendors that need access to perform their job function.
- 3) Where practical, all visitors should be restricted from areas where files or systems containing PII and/or sensitive company data are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files or systems containing PII and/or sensitive company data are stored.
- 4) A clean desk policy will be implemented and includes the following: All employees are prohibited from keeping unsecured paper files containing PII and sensitive company data in their work area when they are not present (e.g. lunch breaks). At the end of the day, all files containing PII and/or sensitive company data are to be stored in a locked filing cabinet, desk drawer or other locked location. Any systems that store or access PII and/or sensitive company data should be closed or access should be terminated (i.e. system logoff).
- 5) The Security Officer shall maintain a secured and confidential master list of all lock combinations, passcodes, and keys. The list will identify which employee possess keys, keycards, or other access devices and that only approved employees have been provided access credentials.

- 6) Where practical, all visitors who are expected to access areas other than common space or are granted access to office space containing PII and/or sensitive company data should be required to sign-in with a Photo ID at a designated reception area where they will be assigned a visitor's ID or guest badge unless escorted at all times. Visitors must be escorted or accompanied by an approved employee in any area where files containing PII and/or sensitive company data are stored.