EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. Purpose

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. Definitions

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy. Erie 1 BOCES will provide Vendor with a copy of its policy and Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA https://uploads.panopto.com/2020/12/16151445/Panopto-Technical-infrastructure-2021.pdf

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor ______will _X____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. Additional Statutory and Regulatory Obligations

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **<u>Notification of Breach and Unauthorized Release</u>**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

ERIE 1 BOCES

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

DocuSigned by:
Will Wyatt
B2E163D5879A4D4...

Signature

Will W□att

Printed Name

Chief Sales Officer

Title

Ma□ 31, 2022

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND PANOPTO, INC.

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Panopto, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

Video Content Management Software

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: NA

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on May 1, 2022 and expires on June 30, 2025.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

Panopto™

Written Information Security Plan

The objectives of this comprehensive Written Information Security Plan ("WISP") are to define, document, and support the implementation and maintenance of the administrative, technical, operational, and physical controls Panopto, Inc. ("Panopto") has adopted to protect the Confidential Information it collects, creates, uses, and maintains.

1. Purpose

The purpose of this WISP is to:

- Ensure the security, confidentiality, integrity, and availability of Confidential Information and the systems maintained by Panopto to collect, create, process, and store that Confidential Information;
- Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information;
- Protect against unauthorized access to or use of Panopto-maintained information systems or Confidential Information that could result in substantial harm or inconvenience to the Company or any customer or employee; and
- Define an information security program that is appropriate to Panopto's size, scope, and business requirements; its available resources; and the risk to Confidential Information that Panopto owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

2. Scope

This WISP applies to all employees, contractors, officers, directors, vendors, and others ("Personnel") who have access to Panopto data and to the systems used to collect, process, store, or maintain Confidential Information. It applies to any records that contain Confidential Information in any format and on any media, whether in electronic or paper form.

For purposes of this WISP, "Confidential Information" means data that:

- Panopto, a customer, or a business partner considers to be confidential or proprietary; or
- If accessed by or disclosed to unauthorized parties, could cause significant or material harm to Panopto, or its employees, customers, or business partners.

Confidential Information includes, but is not limited to, Personal Data and Sensitive Personal Data. "Personal Data" means any data, whether alone or in conjunction with other data, that relates directly or indirectly to a natural and identifiable individual. This includes, for example: names, birthdates or age, identification numbers such as a US Social Security Number, subscriber identification number and similar identifiers, email addresses, location and physical or mailing addresses, telephone numbers, IP addresses, and other online identifiers.

"Sensitive Personal Data" or "Special Category Personal Data" requires further special handling and has restrictions on its collection, use, and processing. Sensitive Personal Data includes data that may reveal an individual's racial or ethnic origin, political opinion or affiliation, religious or philosophical beliefs, trade union membership, health information or medical conditions, sexual orientation, and also includes genetic and biometric data (fingerprints, iris scans, facial recognition markers, and similar when processed to individually identify a person).

3. Information Security Risk and Compliance Manager

Panopto has designated the Information Security Risk and Compliance Manager ("Information Security Manager") to implement, coordinate, and maintain this WISP. The Information Security Manager is responsible for:

- Implementation of this WISP, including:
  - Leading a companywide cross-functional Information Security Council to govern the WISP;
  - Assessing internal and external risks to Confidential Information and Company information systems and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);
  - Coordinating the development, distribution, and maintenance of information security policies and standards (see Section 5);
  - Coordinating the design, implementation, and maintenance of appropriate administrative, technical, and physical controls to protect Confidential Information and information systems (see Section 6);
  - Monitoring compliance by vendors and service providers that access or maintain Confidential Information or Company information systems on behalf of Panopto (see Section 7);
  - Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 8);
  - Defining and maintaining incident response procedures (see Section 9); and
  - Establishing and maintaining enforcement policies and procedures for this WISP, in collaboration with Panopto's Employee Experience team and senior management (see Section 10).
- Employee, contractor, and other stakeholder training, including:
  - Providing regular training regarding this WISP, Panopto's controls, and relevant information security policies and standards for all Personnel who have or may have access to Confidential Information;
  - Ensuring that training attendees formally acknowledge their receipt and understanding ofthe training and related documentation; and
  - Retaining training and acknowledgment records.
- Reviewing the WISP and the security measures defined herein at least annually, or whenever there is a material change in Panopto's business practices, or external factors that may reasonably affect the security, confidentiality, integrity, or availability of records or information systems containing Confidential Information (see Section 11);
- Defining and maintaining a process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or Panopto's information security policies; and
- Periodically reporting to the Information Security Council on the status, effectiveness of, and updates to the information security program.

4. Risk Assessment

Panopto has developed and maintains a documented risk assessment process, conducted at least annually, or whenever there is a material change in Panopto's business practices or external factors that may affect the security, confidentiality, integrity, or availability of records or information systems containing Confidential Information. The risk assessment process includes:

- Identifying reasonably foreseeable internal and external threats to the security, confidentiality, integrity, or availability of any electronic, paper, or other records, or to any Company-maintained information system, containing Confidential Information;
- Assessing the likelihood and potential damage that could result from such threats, taking into consideration the sensitivity of the Confidential Information;
- Evaluating the sufficiency of relevant policies, standards, systems, and controls in place to mitigate such risks, in areas that include, but may not be limited to:
  - Employee, contractor, and other stakeholder training and management;
  - Employee, contractor, and other stakeholder compliance with this WISP and related policies;
  - Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and
  - Panopto's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

Following each risk assessment, Panopto shall:

- Design, implement, and maintain reasonable and appropriate controls to mitigate identified risks;
- Reasonably and appropriately address any identified gaps; and
- Regularly monitor the effectiveness of Panopto's controls, as specified in this WISP (see Section 8).

5. Information Security Policies and Standards

As part of this WISP, Panopto has developed and will maintain and update information security policies and standards, consistent with the NIST SP 800-53 control families, governing:

- Access control;
- Awareness and training;
- Audit and accountability;
- Assessment, authorization, and monitoring;
- Configuration management;
- Business continuity and disaster recovery planning;
- Identification and authentication;
- Incident response handling and communications;
- Information classification and handling;
- Information system maintenance;
- Media protection;
- Physical and environmental protection of information systems;
- Information security program planning and management;
- Personnel security;
- Privacy and data protection;

- Risk assessment;
- System and services acquisition;
- System and communications protection;
- System and information integrity; and
- Supply chain risk management

6. Common Controls

Panopto has developed, implemented, and will maintain commercially reasonable administrative, technical, operational, and physical controls to protect the security, confidentiality, integrity, and availability of Confidential Information and the information systems that Panopto owns or maintains on behalf of others, consistent with Panopto's size, scope, and business requirements; its available resources; and the risk to Confidential Information that Panopto owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

- Panopto's common administrative controls include, but are not limited to:
    - Designating one or more employees to coordinate the information security program (see Section 3);
    - Identifying internal and external risks, assessing whether existing controls adequately mitigate the identified risks, and developing, implementing, and maintaining necessary remediation steps where necessary to augment or update existing controls (see Section 4);
    - Training employees in security program practices and procedures, including appropriate data classification and handling, privacy and protection of Personal Data (see Section 3);
    - Selecting vendors and service providers that maintain appropriate controls, and requiring vendors and service providers to maintain controls by contract (see Section 7); and
    - Updating the information security program in consideration of business changes or new circumstances or threats to the confidentiality, integrity, or availability of Company-maintained information systems or Confidential Information (see Section 11);
- Panopto's common technical and operational controls extend to its corporate and production networks and information systems. They include, but are not limited to:
    - Secure user authentication protocols such as:
        - Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;
        - Restricting access to active users and active user accounts only, including preventing terminated employees or contractors from accessing systems or records; and
        - Blocking access to a user account after multiple unsuccessful attempts to gain access or placing limitations on access to the affected system.
    - Secure access control measures such as:
        - Restricting access to records and files containing Confidential Information to those with a need to know to perform their duties;
        - Assigning unique identifiers and passwords (or other authentication means) to each user with computer or network access that are reasonably designed to maintain security; and

        - Changing vendor-supplied default passwords.
    - Encryption of all Confidential Information traveling wirelessly or across public networks.
    - Encryption of all Confidential Information stored on laptops or other portable or mobile devices, and to the extent technically feasible, Confidential Information stored on any other device or media.
    - Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to Confidential Information or other attacks or system failures.
    - Regular vulnerability scans and third-party penetration tests of systems that contain Confidential Information;
    - Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) Confidential Information.
    - Reasonably current system security software that (1) includes malicious software ("malware") protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.
- Panopto's common physical controls include, but are not limited to:
    - Defining and implementing reasonable physical security measures to protect areas where Confidential Information may be accessed, including reasonably restricting physical access and storing records containing Confidential Information in locked facilities, areas, or containers;
    - Preventing, detecting, and responding to intrusions or unauthorized access to Confidential Information, including during or after data collection, transportation, or disposal; and
    - Secure disposal or destruction of Confidential Information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

7. Vendor and Service Provider Oversight

Panopto oversees its vendors and service providers that have access to or otherwise create, collect, process, store, or maintain Confidential Information on its behalf to ensure their compliance with Panopto Information Security standards and applicable laws, by:

- Evaluating the vendor's or service provider's ability to implement and maintain appropriate security measures;
- Requiring by contract that the vendor or service provider implement and maintain reasonable security measures;
- Monitoring and auditing the vendor's or service provider's performance and regularly verifying ongoing compliance.

8. Program Monitoring

Panopto regularly tests and monitors the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of Confidential Information. Panopto shall reasonably and appropriately address any identified gaps.

9. Incident Response

Panopto has established and will maintain procedures regarding information security incident response planning, testing, communications, and remediation (see Section 5).

10. Enforcement

Noncompliance with this WISP shall result in disciplinary action, up to and including termination of access to information resources or of employment or partnership, in accordance with Panopto's human resources, employment, and procurement policies.

11. Program Review

Panopto reviews this WISP and the security measures defined herein, at least annually, or as needed due to a material change in Panopto's business practices, external factors, or legal requirements that may impact the security, confidentiality, integrity, or availability of company-maintained information systems or records containing Confidential Information. Panopto retains documentation regarding such program reviews, including any identified gaps and action plans.

12. Related Policy

3.0 Program Management Policy

13. Version History

Version	Date	Author	Comment
1.0	6/15/2020	Matt Pierce	Initial draft
1.1	9/16/2020	Matt Pierce	Incorporate comments from Legal
	9/28/2020		Approved by Information Security Council