Augustana College Written Information Security Program

# 1.0 Program Statement

The Augustana College Written Information Security Policy (“WISP”) is intended as a set of comprehensive guidelines and policies designed to safeguard confidential and restricted data maintained at the College, and to comply with applicable laws and regulations on the protection of Personal Information and Nonpublic Financial Information, as those terms are defined below, found in records and in systems owned by the College. 

# 2.0 Overview & Purpose

This written information security program (WISP) was implemented to comply with regulations issued by the State of Illinois; and by the Federal Trade Commission [16 CFR Part 314]; and with our obligations under the financial customer information security provisions of the federal Gramm-Leach-Bliley Act (“GLB”) [15 USC 6801(b) and 6805(b)(2)]; and the European General Data Protection Regulation as applicable.

In accordance with these federal, state, and international laws and regulations, Augustana College is required to take measures to safeguard personally identifiable information*,*including financial information, and to provide notice about security breaches of protected information at the college to affected individuals and appropriate state agencies.

Augustana College is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who work or study at the College.  Augustana College has implemented a number of policies to protect such information, and the WISP should be read in conjunction with these policies that are cross-referenced at the end of this document.

The purposes of this document are to:

1. Establish an adaptive and comprehensive information security program for Augustana College with policies designed to safeguard sensitive data that is maintained by the College, in compliance with federal, state, and international laws and regulations as applicable;
2. Establish employee responsibilities in safeguarding data according to its classification level; and
3. Establish administrative, technical and physical safeguards to ensure the security of sensitive data.

# 3.0 Scope

This Program applies to all Augustana College employees, whether full- or part-time, including faculty, administrative staff, contract and temporary workers, hired consultants, interns, and student employees, as well as to all other members of the Augustana College community (hereafter referred to as the “Community”).  This program also applies to certain contracted third-party vendors (see section 4.6 for further information).  The data covered by this Program includes any information stored, transported, accessed or collected at the College or for College operations.  The WISP is not intended to supersede any existing Augustana College policy that contains more specific requirements for processing and safeguarding certain types of data. If such policy exists and is in conflict with the requirements of the WISP, the other policy may take precedence.

# 4.0 Definitions

**Augustana Community:** The collection of students, employees, alumnae, volunteers, business partners, and organizations who access, collect, extract, transport, store, analyze, view, and manage data on the behalf of Augustana College.

**Data:** For the purposes of this document, data refers to information stored, transported, accessed, provisioned, derived from, recorded or otherwise collected for the College about members of the College community*.*

**Personal Information:** Personal Information (“PI”) is the first name and last name or first initial and last name of a person in combination with any one or more of the following:

* Social Security number
* Driver’s license number or state-issued identification card number
* Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person’s financial account, with or without any required security code, access code, personal identification number, or password.
* Date of Birth
* Medical information
* Health insurance information
* Unique biometric data
* Username or email address in combination with a password or security question answer that would permit access to an online account
* For the purposes of this Program, PI also includes passport number, alien registration number or other government-issued identification number.

# 4.2 Data Classification

All data covered by this Program should be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level.

* **Confidential**

Confidential data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a significant level of risk to Augustana College or the college community. Confidential data includes all data that is protected by 1) applicable federal, state, local, and international law or regulation; or 2) College policy or operations. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration or disclosure.

* **Restricted**

Restricted data refers to all other personal and institutional data where the loss of such data could harm an individual’s right to privacy or negatively impact the finances, operations or reputation of Augustana College. Any non-public data that is not explicitly designated as confidential or public should be treated as restricted data.

Restricted data includes data protected by the Family Educational Rights and Privacy Act (FERPA), referred to as student education records. This data also includes, but is not limited to, donor information, research data on human subjects, intellectual property (proprietary research, patents, etc.), College financial and investment records, employee salary information, or information related to legal or disciplinary matters.

Restricted data should be limited to access by individuals who are employed by or matriculate at Augustana College and who have legitimate reasons for accessing such data, as governed by FERPA, or other applicable law or College policy. A reasonable level of security should be applied to this classification to ensure the privacy and integrity of this data.

* **Public (or Unrestricted)**

Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to Augustana College or members of the Augustana College community.  Public data should be explicitly identified as such through College policy as well as governing federal, state, and local laws and regulations.

# 5.0 Roles and Responsibilities

**Information Technology Services:** ITS staff shall be responsible for all data stored centrally on the College’s servers and administrative systems, and are responsible for the security of such data.  For distributed data stored on departmental servers, the department head or their designee shall be responsible, and ITS and the department share joint responsibility for securing the data under the direction of the College’s designated data security coordinator.

**Department Leaders:** Department heads will alert Human Resources and Information Technology Services at the conclusion of a contract for individuals that are not considered Augustana employees in order to terminate access to their Augustana College network and service accounts.

**The Augustana community:** The campus community shares responsibility for maintaining the privacy and integrity of all Confidential, Restricted, or Public data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All members of the Augustana community are required to access, store and maintain records containing Confidential, Restricted, or Public data in compliance with this Program.

* **Data Trustee:** Data trustees are the senior college officials (or their designees) who have planning and Program-level responsibility for data within their functional areas and management responsibilities for defined segments of institutional data. Responsibilities include assigning data stewards, participation in the establishment of protective policies, and promoting data-resource management for the good of the entire college. These are the Provost/VP-level officials.
* **Data Steward:** Data stewards are college officials having direct operational-level responsibility for information management - usually department heads or directors. Data stewards are responsible for data access and policy implementation issues. Examples of these are the College Registrar, Director of Human Resources, Controller, etc.
* **Data Custodian:** The custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes; granting access privileges to system users as authorized by data trustees or their designees (usually the data stewards); and implementing and administering controls over the information. In many cases, Information Technology Services is the data custodian but not always. If the data custodian is a third-party service provider, extra steps are required to ensure the secure transmission, storage, and handling of the college's confidential information or covered data. Security provisions and steps should be clearly outlined in a vendor service agreement or contract.
* **Data User:** Data users are individuals who need and use college data as part of their assigned duties or in fulfillment of assigned roles or functions within the college community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.
* **Chief Information Security Officer (CISO):** The CISO helps coordinate security efforts and assists with the dissemination of policies, procedures and guidelines to the college community; helps raise information security awareness through education and training; helps develop risk management plans and incident response procedures; analyzes security incidents; and develops a set of tools to assist investigation and compliance. For Augustana, the role of Information Security Officer is addressed within the role and responsibilities of the Chief Information Officer.
* **Incidence Response Team (IRT):** In order to coordinate response to and resolution of security incidents, the College has established an Incidence Response Team. The IRT includes General Counsel, the Vice President of Finance, and the Chief Information Officer. The team coordinates the resources necessary to complete the phases of addressing a data security incident: Discover, Investigate, Respond and Closure. Review the Incidence Response Plan for further details.

# 6.0 Identification and Assessment of Risks to College Information

Augustana College recognizes that it has both internal and external risks to the privacy and integrity of College information. These risks include, but are not limited to:

* Unauthorized access of Confidential data by someone other than the owner of such data
* Compromised system security as a result of system access by an unauthorized person
* Interception of data during transmission
* Loss of data integrity
* Physical loss of data in a disaster
* Errors introduced into the system
* Corruption of data or systems
* Unauthorized access of Confidential data by employees
* Unauthorized requests for Confidential data
* Unauthorized access through hard copy files or reports
* Unauthorized transfer of Confidential data through third parties
* Unauthorized access introduced via supply chain solution providers

Augustana College recognizes that this may not be a complete list of the risks associated with the protection of Confidential or Restricted data. Since technology is not static, new risks are created regularly. Accordingly, ITS will work with and monitor advisory groups such as the EDUCAUSE Security Institute, the SANS institute, National Institute of Science and Technology as well as other resources known for identification and mitigation of cyber risk.

# 7.0 Policies for Safeguarding Confidential Data

To protect College data classified as Confidential, the following procedures and guidelines have been developed that relate to access, storage, transportation and destruction of records.

**Access & Storage**

* Only those employees or authorized third parties requiring access to Confidential data in the regular course of their duties are granted access to this data, including both physical and electronic records.
* To the extent possible, all electronic records containing Confidential data should only be stored on the College’s on-campus secure network storage and not on local machines or unsecured servers.
* Confidential data must not be stored on cloud-based storage solutions that are unsupported by the College (including DropBox, Microsoft OneDrive, Apple iCloud, etc.).
* Members of the Community are strongly discouraged from storing Confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives).  However, if it is necessary to transport Confidential data electronically, the mobile device containing the data must be encrypted.
* Paper records containing Confidential data must be kept in locked files or other secured areas when not in use.
* Upon termination of employment or relationship with Augustana College, electronic and physical access to documents, systems or other network resources containing Confidential data is immediately terminated.

**Transporting Confidential Data**

* Members of the Augustana community are strongly discouraged from removing records containing Confidential data off campus.  In cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data.  Under no circumstances are documents, electronic devices, or digital media containing Confidential data to be left unattended in any unsecure location.
* When there is a legitimate need to provide records containing Confidential data to a third party outside Augustana College, electronic records shall be password-protected and/or encrypted, and paper records shall be marked confidential and securely sealed.

**Destruction of Confidential Data**

* Records containing Confidential data must be destroyed once they are no longer needed for business purposes, unless state or federal regulations require maintaining these records for a prescribed period of time.
* Paper and electronic records containing Confidential data must be destroyed in a manner that renders the personal information unreadable, unusable, and undecipherable.  The Illinois Information Security Act (815 ILCS 530/40) specifies the manner in which records containing PI must be destroyed.

**Traveling Abroad with Students’ Personal Information**

* In the event that transmission of student passport information is required by the hotel or program abroad in advance of the travel, only the relevant information requested (e.g., Name, Passport Number, Date of Expiry, and Date of Birth) will be provided, not complete copies of the passport images.  This information should first be transmitted via fax or through eFax Secure website (SSL), provided that the Augustana College department arranging the travel confirms the accuracy of the fax number by sending an initial confirmation message before the actual data.
* Faculty/staff who need to retain these passport numbers for arranging travel will store this data in spreadsheets that are saved on the College’s secure file server.  Any spreadsheets containing student passport information should be routinely deleted by the spreadsheet owner when no longer needed.
* Faculty/staff who are traveling with the students abroad that need student passport and visa information for hotel check-in will keep a paper record on their person that contains relevant information (such as the passport and visa numbers and their expiry dates) and the last names of the students only. Faculty/staff must not retain or travel with copies of student passports.
* In extreme circumstances involving travel to a remote location where access to technology would be limited and would prohibit retrieval of a lost passport, a program director may request an exemption to this Program allowing for him or her to retain copies of the students passports during travel.  This request will be made to the Chief Information Officer for approval.  If the request is approved, the program director will sign the “[Faculty/Staff Agreement for Traveling with Secure Data](https://docs.google.com/a/wellesley.edu/forms/d/1BhXIwCxoxUoJ2il8Fh4VZsbNb84y4bE82x_wyOyaH9s/viewform)” to acknowledge their understanding of the WISP and their responsibilities in protecting the passports.  The program director also agrees to alert the office of Academic Affairs, Dean of Students office, and Information Technology Services immediately if the copies of passport are lost.

# 8.0 Policies for Safeguarding Restricted Data

* Access to Restricted Data should be limited to members of the Community who have a legitimate business need for the data.
* Restricted Data can be stored on Google Apps, College file servers in designated shared personal or office folders or in encrypted portable devices.
* Restricted data may be stored on cloud-based storage solutions that are unsupported by the College as long as they are in compliance with the requirements of any laws governing the protection of such data (e.g., FERPA).
* Documents containing Restricted Data should not be posted publicly.

# 9.0 Password Requirements

In order to protect College data, all members of the Community must select unique passwords following these guidelines:

* Passwords will expire every 120\* (approx. one semester)
* You cannot use one of your last 20 passwords
* Passwords have a minimum of 14 characters and a maximum of 20 characters
* You cannot use your name in your password
* Some special characters (like spaces or emojis) cannot be used
* Passwords must meet 3 of these 4 requirements:
* At least 1 upper case letter
* At least 1 lower case letter
* At least 1 number
* At least 1 special character
* Users will need to use the change their password at myaccount.augustana.edu or on a lab Windows PC on login (for expired accounts) or with ctrl-alt-del - “change password” (for unexpired accounts).
* Members of the community must protect the privacy of their passwords. Passwords must not be shared with others. If an account or password is suspected to have been compromised, all passwords should be changed immediately and the incident reported to the Augustana College Help Desk.

# 10.0 Third-Party Vendor Agreements Concerning Protection of Personal Information

Augustana College exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for PI provided by the College to them.  The primary budget holder for each department is responsible for identifying those third parties providing services to the College that have access to PI. All relevant contracts with these third parties are reviewed and approved by the Augustana College Purchasing Department, General Counsel and Chief Information Officer to ensure the contracts contain the necessary language regarding safeguarding PI. It is the responsibility of the primary budget holders to confirm that the third parties are required to maintain appropriate security measures to protect PI consistent with applicable laws and regulations.

# 11.0 Computer system safeguards

Technology Support Services staff monitor and assess safeguards on an ongoing basis to determine when enhancements are required.  The College has implemented the following to combat external risk and secure the College network and systems containing Confidential Data:

Secure user authentication protocols:

Unique passwords are required for all user accounts; each employee receives an individual user account.

Server accounts are locked after multiple unsuccessful password attempts.

Augustana Active Directory or AD linked accounts are locked after multiple unsuccessful password attempts.

Computer access passwords are disabled upon an employee’s termination.

User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.

Secure access control measures:

Access to specific files or databases containing Confidential Data is limited to those employees who require such access in the normal course of their duties.

Information Technology Services staff perform regular internal network security audits to all server and computer system logs to discover, to the extent reasonably feasible, possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of College data.

Operating system patches and security updates are installed to all servers on a regular basis.

Antivirus and anti-malware software is installed and kept updated on all workstations.

# 12.0 Employee Training

All employees are required to complete the online security training on an annual basis.  Any faculty, student or contract employee that has access to PI is also required to complete this yearly training.

# 13.0 Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the CIO.  The CIO will contact the Data Incident Response Team who will convene a meeting and develop an appropriate response plan as soon as possible. The Data Incident Response Team is responsible for coordinating appropriate actions in their response to the breach. The Incident Team will document all breaches and subsequent responsive actions taken.  All related documentation will be stored in the Business Office vault.

For more information about incident response, including specific procedures for responding to a breach, see the Augustana Incidence Response Plan

# 14.0 Enforcement

Any employee or student who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Confidential or Restricted data without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, which may include termination in the case of employees and expulsion in the case of students.

# 15.0 Policies cross-referenced.

The following Augustana College policies provide advice and guidance that relates to this Program:

[Acceptable Use Policy](https://www.augustana.edu/about-us/offices/ITS/Policies)

Data Incident Response Plan

Electronic Content Stewardship Policy

Employee Confidentiality Policy

[FERPA Policy](https://www.augustana.edu/academics/registrar/privacy)

HIPAA Privacy Policy

Identity Theft Prevention Policy ("Red Flag Rules")

Password [Policy](https://www.augustana.edu/about-us/offices/ITS/Policies/Passwords)

Records Management Policy

Remote Access Policy

# 16.0 Review and Revisions:

This Written Information Security Program was implemented XXXXXXX.

The College will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.