Curry College

Written Information Security Program (WISP)

Last Edited: June 7, 2019

1.0 Policy Statement

The Curry College Written Information Security Program (WISP) is intended as a set of basic safeguards to protect the confidentiality, integrity, and availability of sensitive information collected and maintained by the College, and to comply with applicable laws and regulations on the protection of that paper and electronic data while at rest in databases, spreadsheets, archive, storage devices, paper, cloud storage, backups, flash storage, laptops and portable devices or in motion through wireless, paper in transport, the internet or private network.

2.0 Overview & Purpose

The information security program outlines the administrative, technical and physical safeguards to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle sensitive information.

The WISP was implemented to comply with the following regulations (not an exhaustive list):

- Standards For The Protection Of Personal Information Of Residents Of The Commonwealth, 201 CMR 17.00
- Massachusetts regulations to safeguard personal information, M.G.L. c. 93H *et seq.* and 940 CMR 27.00
- Federal Trade Commission, Privacy of Consumer Financial Information & Standards for Safeguarding Customer Information, 16 CFR Part 313 & 314
- Financial customer information security provisions of the federal Gramm-Leach-Bliley Act (GLB), 15 USC 6801(b) and 6805(b)(2)
- Health Insurance Portability and Accountability Act (HIPPA), Pub. Law 104-191 and related regulations
- Family Education Rights and Privacy Act (FERPA), 20 U.S.C. 1232g (and related regulations)
- Fair Credit Reporting Act (FRCA), 15 U.S.C. 1681 (and related regulations)
- Payment Card Industry Security Standard Council (PCI DSS)
- General Data Protection Regulations (GDPR)

In accordance with these federal and state laws and regulations, Curry College is required to take measures to safeguard sensitive data, including financial information, and:

- ensure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of such records;
- protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer; and
- provide notice about security breaches of sensitive information at the college to affected individuals and appropriate state agencies.

Curry College is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who work and study at the College. Curry 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.

3.0 Scope

This Program applies to all Curry College employees, whether full- or part-time, including faculty, administrative staff, union staff, contract and temporary workers, consultants, interns, and student employees, third party service providers, as well as to all other members of the Curry College community (Community). This program does not apply to volunteers of Curry as they are prohibited from having any contact with sensitive data. The data covered by this WISP includes any information collected, stored, maintained, processed, owned, and licensed by Curry College in connection with the mission, partnerships, or employment. The WISP is not intended to supersede any existing Curry College policy that contains more specific requirements for safeguarding certain types of data, except in the case of Personal Information and Nonpublic Financial Information, Protected Health Information, and FERPA protected data as defined below. If such policy exists and is in accordance with the requirements of the WISP, the more restrictive policy is controlling.

3.1 Data Types Protected by Laws and Regulations

Family Education and Rights Privacy Act (FERPA) Protected Data: FERPA protected data, as defined by FERPA is the educational record of a student in whatever medium (handwritten, print, tape, film, disk, and etc.) that are in the possession of any school official (includes a faculty, deans, president, provost, board member, trustee, registrar, counselor, admissions officer, attorney, accountant, human resources professional, information systems specialist, and support or clerical personnel).

Nonpublic Personal Information (NPI): Any personally identifiable financial information; provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution. NPI does not include publicly available information. NPI does include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.

Payment Card Industry (PCI) Security Standard: The primary account number (PAN) of a credit card, debit card, or bank account number in combination with any one or more of the following:

- cardholder name;
- service code; or
- expiration date

Personal Information (PI): The first name and last name or first initial and last name of a person (including a corporation, association, partnership or other legal entity) in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- 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.

For the purposes of this Program, PI also includes passport number, alien registration number or other government- issued identification number.

Personal Data (PD) of Person(s) Located in European Union (EU) and Member States within the European Economic Area (EEA) (regardless of citizenship): Any information relating to an identified or identifiable natural person (data subject) within the EU and EEA (which, in addition to EU Member States, includes Iceland, Norway, Liechtenstein, United Kingdom and Switzerland); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (IP address or cookie) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Protected Health Information (PHI): Any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

Sensitive Information: Data that is protected by this Program and the following federal or state laws or regulations: 201 CMR 17.00, **[PI**] M.G.L. c93H, s 2 **[NPI]**, 16 CFR Part 313 & 314 **[NPI]**, GLB 15 USC 6801(b) and 6805(b)(2) **[NPI]**, and HIPPA Pub.L. 104–191 **[PHI]**, 20 U.S.C. 1232g **[FERPA],** Payment Card Industry Data Security Standard [**PCI**], and GDPR **[PD]**

3.2 Data Classification

Data covered by this Program will be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level. This Program is explicitly intended to meet legal requirements relating to the protection of Sensitive Data.

Sensitive: Unauthorized access, use, alteration or disclosure of such data could present a significant level of risk to Curry College or the Community or violate applicable laws or regulations. Sensitive data should be treated with the highest level of restrictions to ensure the privacy of that data and prevent any unauthorized access, use, alteration or disclosure.

Confidential/Private: Proprietary or business information that may be exchanged within the College or with authorized vendors or other third parties, but represents a reputational or business risk if disclosed. As examples, such data might include College financial information, donor records or vendor lists.

Public: The least sensitive data used by the College and would cause the least harm if disclosed. As examples, such data might include directory information, website information and admissions recruiting materials.

4.0 Written Information Security Program

4.1 Responsibilities

Institutional Information Security Workgroup: The Institutional Information Security workgroup, chaired by the College's CIO has overall responsibility for this Program and through delegation and oversight is responsible for implementation, compliance, oversight, ensuring violations are corrected, assuring regular and appropriate training, overseeing audits, and in collaboration with the College Council evaluating the ability of Third Party Services provider to protect Curry College sensitive information.

Division/Department Heads: Each department that collects and maintains sensitive information will identify a person in the department responsible for adherence to this policy and the implementation of procedures required to protect the confidentiality, integrity, and availability of sensitive information.

The Community: All members of the Curry Community are responsible for maintaining the privacy and integrity of all sensitive data they come in contact with, and must protect the data from unauthorized use, access, disclosure or alteration.

4.2 Administrative Safeguards

Administrative safeguards focus on two areas: personnel and business practices**.** Administrative safeguards should never be circumvented by anyone in the Community.

4.2.1 Security Awareness

A copy of the WISP will be distributed to each employee, student or temporary employee, third party service provider, vendor or Curry affiliate when access to sensitive data is requested. Upon receipt of the WISP, acknowledge in writing or electronically that he/she has received a copy of the Program, access to the sensitive data will be provisioned.

Information Technology Services (ITS) is responsible for regular ongoing training and retraining of employees, student or temporary workers, third party service provider, vendors or Curry affiliates with access to sensitive information will be offered by Curry. Data Owners (as defined in section 4.2.4 of this Program), or appointed designees, are responsible for updating their area and the CIO on new and changing regulations covering data they own. The Data Owner will communicate the name of the appointed designee, if assigned, in writing to the CIO.

4.2.2 Collecting Sensitive Data

The amount of sensitive information collected must be limited to that amount reasonably necessary to accomplish the Curry's legitimate educational and business purposes, or necessary to comply with other state or federal regulations.

Credit card holder data defined by the Payment Card Industry Data Security Standard (PCI DSS) including a credit card number with or without any required security code or expiration date are never to be written down on paper, form, or stored on a system that is not PCI DSS compliant.

The collection and processing of Personal Data of natural persons within the European Union and European Economic Area, regardless of nationality or residence is highly regulated and is outlined in the Curry Data Protection Regulation (GDPR) Privacy Notice.

4.2.3 Storing Sensitive and Confidential/Private Data

Electronic records containing sensitive, confidential/private data should only be stored on the Curry College network, approved systems and media, and paper in secured location, and not on **any** desktop computers, laptops, mobile devices, personal smart phones, external hard drives, USB drives, or unapproved cloud storage.

Questions about the College's Record Retention and Destruction Policy may be directed to the Chief Financial Officer.

4.2.4 Access to Sensitive Data

Access to records containing sensitive data shall be based on the principle of least privilege and need-to-know such information in order to accomplish the Curry's legitimate educational and business. The identity of a person must be verified before access is granted.

All sensitive data at the College is assigned a Data Owner and Administrator according to data type.

Data Owner: Has control over data and is responsible for approving requests for access to such data.

Administrator: Has technical control over Enterprise Application (EA) and Enterprise Infrastructure (EI) data within the Tech Center, and is responsible for the technical security of such data.

Type of Data	Data Owners & Appointed Designees	Administrators (System & Network)
Faculty	Provost	EA and EI Teams within Tech Center
Staff	VP of Human Resources	EA and EI Teams within Tech Center
Student	VP of Student Affairs/Dean, Registrar, VP of Admission/Dean, and Associate VP of Finance for SFS, Associate VP of Academic Affairs	EA and EI Teams within Tech Center
Alumni	VP for Advancement	EA and EI Teams within Tech Center

*The data owner may appoint a designee to serve in their place.

4.2.5 Internal and External Risk

Risk Analysis: Division/Department heads will perform an annual risk analysis or whenever there is a material change in business practices that may impact sensitive information, which will provide an assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of sensitive information as well as a review of compliance to this Program.

Risk Management: Division/Department heads will implement measures to reduce computer risks and vulnerabilities, including identifying and documenting potential risks and vulnerabilities that could impact systems collecting and storing sensitive information as well as the proper disposition of sensitive information. Risk Management reports will be sent to the CIO annually.

Annual WISP Audit: Data Owners, or appointed designees, will perform an annual update inventory of systems and devices containing sensitive data, review of access controls within their area to assure access supports principle of least privilege and need-to-know.

4.2.6 Employees and Third-Party Service Providers

- Human Resources will inform ITS of an employee's change of status or termination as soon as is practicable but before an employee's departure date from the College. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to College data.
- Third party service providers with whom the College shares sensitive information or who has incidental access to sensitive information within the scope of their work shall either sign an agreement acknowledging this policy and assuring to keep such information protected and confidential, or submit a copy of their company policy on confidentiality and protection of sensitive information for review and approval by the College's Counsel. Division/Department heads will alert ITS via email at the conclusion of a contract for individuals that are not considered Curry College employees in order to terminate access to their Curry College accounts.

4.3 Physical Safeguards

Physical safeguards focus on physical measures to protect sensitive information. Physical safeguards should never be circumvented by anyone in the Community.

Secure Paper Files: Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall kept in locked files or other secured areas when unattended, not in use, and at the end of the work day.

Limit Access to Printouts: Fax machines, printers, multifunction, and other devices receiving or printing sensitive information shall be located in secure areas, not accessible to the general public, that can be locked at night. When printing or receiving faxed sensitive data, immediately retrieve the fax transmission from the fax machine.

Disposition of Paper Records: Paper records with sensitive data will be disposed of in a locked secure bin or in a manner that complies with M.G.L. c. 93I.

Sensitive Information Collection: Sensitive information including credit card holder data defined by the Payment Card Industry Data Security Standard (PCI DSS) including a credit card number with or without any required security code or expiration date are never to be written down on paper or requested on a College paper form or non-secure form over the internet or private network.

Device and Media Controls: Devices with sensitive information stored (laptops, computers, fax machines, copiers, multifunction devices, etc.) shall be wiped before being disposed. Devices with sensitive information may not be transported through campus mail or other mail or package delivery companies.

Physical Safeguards Specific to Departments: Each department shall consider developing procedures that ensure that reasonable restrictions upon physical access to records containing sensitive data are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted.

Facility Access Control: Systems containing sensitive information (servers) will be kept in areas with physical security controls that restrict access.

Contingency Plan: ITS will assure that all systems containing sensitive information have disaster recovery plans in place to respond to an emergency or other occurrence that damages the system.

4.4 Technical Safeguards

Technical safeguards focus on technology (systems, configurations, etc.) to protect sensitive information. Technical safeguards should never be circumvented by anyone in the Community.

Auto-Lock Computer Screens: As a safeguard, all college computers will be programmed to automatically lock (requiring re-entry of a password) after a specified time of no activity.

System Credentials: Credentials for active employees, student or temporary workers, third party service providers, vendors or Curry affiliates with access to sensitive information shall have a minimum length of 10 characters, as recommended by the NIST security framework.

Access Control: Only those employees or authorized third parties requiring access to sensitive data in the regular course of their duties are granted access to this data.

- When systems are available, electronic access to system and files with sensitive data after multiple unsuccessful attempts to gain access shall be blocked.
- Access to sensitive data shall be restricted to active users and active user accounts only.

- Access to electronically stored sensitive information shall be limited to those employees having a unique logon; and re-logon shall be required when a computer has been inactive after a certain period of time.
- Unique usernames (if feasible) and passwords which are not vendor-supplied default passwords, will be assigned to each person and process with access to sensitive information.

Monitoring of Systems: Logs will be enabled and on systems with sensitive information and retained for six months. Reasonable monitoring of exceptions will be put in place, for unauthorized use of or access to sensitive information.

Firewall Protection: There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the sensitive data, installed on all systems processing sensitive data and connected to the internet.

Anti-Virus Software: There must be reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing sensitive information.

Encryption Devices: To the extent operationally feasible, all sensitive information stored on backups, laptops and other portable devices must be encrypted, as must all records and files containing sensitive data transmitted across public networks or wirelessly. Encryption here means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Detection and Prevention: To the extent operationally feasible, a means of detecting and preventing security system failures will be in place.

User Authentication: There must be secure user authentication protocols in place, including:

- Protocols for control of user IDs and other identifiers;
- A reasonably secure method of assigning and selecting passwords;
- Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect**;**
- Restriction of access to active users and active user accounts only; and
- Blocking of access to user identification after multiple unsuccessful attempts to gain access, when possible.

Separate Credit Card Holder Data Traffic: Traffic transporting credit card holder data is segmented so it is separate from the other network traffic.

4.5 Reporting Attempted or Actual Breach of Security

A breach of security is defined as unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information maintained by Curry College.

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of sensitive information, 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 Director of Finance. The Director of Finance and CIO are responsible for coordinating an ad-hoc Data Incident Workgroup which will include appropriate staff from the Tech Center, Finance, Counsel, and the subject department division(s) or department(s) head and determining appropriate actions in their

response to the breach. The Data Incident Workgroup will document the attempts and actual breaches, and subsequent responsive actions taken. All related documentation will be stored in the Finance Office.

5.0 Enforcement

Any member of the Community who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises sensitive 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.

Under federal law, violation of the HIPAA privacy rule may result in civil monetary penalties of up to $250,000 per year and criminal sanctions including fines and imprisonment.

6.0 Appendix

The following Curry College policies & programs provide advice and guidance that relates to this Program:

- CurryNet Acceptable Use Policy
- FERPA Policy
- Record Retention Policy
- Red Flag Rules
- Data Privacy
- Disaster Recovery Program
- Incident Response Plan
- GDPR Program (to be implemented – Spring 2019)

Recurring WISP Undertakings

When	WISP Undertaking	Responsible Area
First day of employment	Distribute WISP to new employees	Human Resources
Prior to Employment	Distribute WISP to student workers	Hiring Manager
When contract is signed	Third party service provider, vendor or Curry affiliate with access to sensitive information	Manager and Director of Finance
March (security awareness month)	Ongoing Security Awareness Training	ITS
March	Annual WISP Audit Due	Data Owner or Appointed Designees
Prior to Date of Change or Term	Notification of employee change of status or termination	Human Resources
Weekly	Review Logs of access to sensitive data in Banner	CIO
Quarterly	Review Firewall change logs	Director of EI
Annually	Review Firewall rules	Director of EI

Sensitive Data Type and Approved Storage Devices Locations

Type of Sensitive Data	Approved Storage of Data	Approved Transport of Data
PI	Curry network drives, Office365 OneDrive & SharePoint, Banner, and Salesforce	FaxFinder, and analog fax
NPI	Curry network drives, Banner, and Salesforce	FaxFinder, and analog fax
HIPPA Protected	Curry network drives, Banner, and Salesforce	FaxFinder, and analog fax
FERPA Protected	Curry network drives, Banner, and Salesforce	FaxFinder, and analog fax
Credit Card Holder Data	Tuition Management Systems (TMS) Payment Processing, GiveCampus, and EventBright	FaxFinder, and analog fax

Written Information Security Program Version Control

Policy Version	Implemented	Date	Replaces	Reviewed By	Date
1.1	Institutional Information Security Workgroup	8/19/19	1.0	Institutional Information Security Workgroup and Executive Team	7/19/19
1.0	Institutional Information Security Workgroup	1/18/19	New	Institutional Information Security Workgroup and Executive Team	11/26/19