Procedure: Security Awareness Program Plan	
Issue Date: 1/1/2023	Revision Date: 1/1/2023
Revision Number: 1.1	NIST Control: AT
Owner: Director of Information Technology	

Contents

THE Wesleyan Way KENTUCKY WESLEYAN COLLEGE	*Written Information Security Program (WISP)*
Effective Date 1/1/2023	Version 1.0

1. Introduction

1.1 Objective

The objectives of this Written Information Security Program (WISP) are to define, document and support the implementation and maintenance of the administrative, technical, and physical safeguards Kentucky Wesleyan College has selected to protect the information it collects, creates, uses, and maintains. This WISP has been developed in accordance with the following security best practices and regulations:

1. NIST Special Publication 800-171 – The NIST Special Publication 800-171 standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls, customized to the needs of individual organization, or parts thereof.
2. Payment Card Industry Data Security Standards (PCI DSS) v3.2 - Contractual obligations addressing the administrative, technical, and physical standards required by payment brands (Visa, AMEX, MasterCard, Discover) for organizations processing payment card transactions.
3. Gramm-Leach-Bliley Act (GLB Act or GLBA) - Federal law enacted in 1999 which requires organizations that loan money to take measures to protect the financial information of individuals.
4. Family Educational Rights and Privacy Act (FERPA) - Federal law enacted in 1974 requiring any school receiving federal funds to protect the privacy of educational records.
5. Health Insurance Portability and Accountability Act (HIPAA) – Enacted by the U.S. Congress in 1996 that mandates covered entities to implement reasonable and appropriate security measures to protect all electronic protected health information (ePHI) against reasonably anticipated threats or hazards.

2. Vision, Mission, and Goals

2.1 Vision

A robust NIST-based security program supported by policies, standards and procedures that address the eighteen (18) NIST security domains.

2.2 Mission

Strengthen the security of Kentucky Wesleyan College environment by implementing a structured security program and ensuring that the relationship between information security and the business objectives of Kentucky Wesleyan College exists and is effective.

2.3 Goals

Deploy security controls to reduce risk for information assets, as defined by specific goals. Achieving these goals requires that Kentucky Wesleyan College:

1. Align information security initiatives with business strategy;
2. Assign ownership and accountability for information security initiatives;
3. Monitor the status and efficacy of information security initiatives; and
4. Institute a process of continuous assessment and improvement.

3. Core Tenants

Kentucky Wesleyan College’s WISP establishes five (5) core tenants, representing the values and assumptions that will be considered when implementing the information security program.

1. Risks are identified and managed in a coordinated and comprehensive way across Kentucky Wesleyan College environment to enable effective allocation of information security resources. This involves promoting efficient and effective use of resources by taking a comprehensive and strategic approach to risk management.

2. Understanding and accounting for dependencies within Kentucky Wesleyan College environment when managing risks is critical to enhancing information security.
3. Information sharing amongst Kentucky Wesleyan College's environment is paramount to gaining knowledge of information security risks.
4. Partnership in implementing Kentucky Wesleyan College's information security program allows for unique perspectives in understanding information security gaps, challenges, and solutions.
5. Information security will be factored into all decisions regarding Kentucky Wesleyan College assets, systems, and networks.

4. Roles and Responsibilities

Commented [RS1]: KWC to discuss governance R&R

4.1 Information Security Leadership

To successfully manage risk across Kentucky Wesleyan College, senior leaders and executives must be committed to making information security a fundamental mission. This top-level, executive commitment ensures that sufficient resources are available to develop and implement an effective, organization-wide security program. Effectively managing information security risk organization-wide requires the following key elements:

- Assignment of risk management responsibilities to senior leaders and executives;
- Ongoing recognition and understanding by senior leaders and executives of the information security risks to organizational information assets, operations and personnel;
- Establishment of the tolerance for risk and communicating the risk tolerance throughout the organization, including guidance on how risk tolerance impacts ongoing decision-making activities; and
- Providing accountability for senior leaders and executives for their risk management decisions.

4.2 Information Security Officer

A senior information security officer will be appointed with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. Responsibilities will include:

- Development, maintenance, and distribution of policies and procedures
- Ensuring responsibilities and assignment for monitoring alerts and incident response processes are understood and performed
- Development, maintenance, and implementation of a security incident response plan.
- Ensure access control processes are defined and implemented
- Ensure all access control processes are monitored

4.3 Information Security Steering Committee

The Information Security Steering Committee provides a number of “soft” benefits, including those gained by the active participation of business leaders in information security decision-making. The Information Security Steering Committee often participates in the following:

1. Establishing goals for the Information Security program;
2. Reviewing and approving Information Security policies and standards;
3. Recommending, reviewing and prioritizing information security initiatives;
4. Communicating information security needs; and
5. Reviewing the effectiveness of the Information Security program and resources
6. Ensuring corrective action plans have been developed and implemented to address risks that are unacceptable to Kentucky Wesleyan College.

The WISP will establish the Information Security Steering Committee and ensure its ongoing operation.

4.4 Resource Optimization

Kentucky Wesleyan College dedicates resources to information security initiatives in an effort to reduce risk, and subsequently meet business objectives. It is understood that these resources are finite and specific, and of the following types:

1. Budget – Funds for information security initiatives will be allocated on an annual basis. Allocated funds are determined by business need, which will be determined by organizational risk.
2. Personnel – The information security team consists of both physical and virtual members, full-time employees, partners, and subcontractors. The number of personnel allocated to information security initiatives is determined by business need, which will be determined by organizational risk. These are allocated and leveraged optimally based on capabilities and availability.
3. Time – The information security team is granted time to complete security initiatives. Schedules for security initiatives are determined by business need, which will be determined by organizational risk.

5. Strategy

5.1 Overview

The key to ensuring that Kentucky Wesleyan College ’s Security program is reasonable and useable is to develop a suite of policy documents that match the intended audience’s business goals and culture. Policies must be practical and realistic. In order to achieve this, it is essential to involve and obtain support from senior management and other stakeholders, as well as from the people who will use the policy as part of their daily work.

The organization will:

- Develop and disseminate information security program standards and an information security plan that provides an overview of the requirements for the security program, a description of the security program management controls and common controls in place or planned for meeting those requirements.

- Establish and maintain organizational policies, standards, and procedures to address all relevant statutory and regulatory requirements, and ensure and support the confidentiality, integrity, and availability of its information assets.
- Make relevant policies, standards, and procedures readily available to all effected workers.
- Conduct a periodic formal review of policies, standards, and procedures and update them, at a minimum, annually.

5.2 Policy Implementation

The Kentucky Wesleyan College has the following three Security Policies formalized or in development stages:

- Acceptable Use Policy – Advises all members of Kentucky Wesleyan College on acceptable and unacceptable behavior involving the organization's resources.
- Data Classification Policy – Describes the process for classification and handling of the organization's data.
- Information Security Policy – Creates provisional compliance requirements for the Kentucky Wesleyan College Information Security Standards. Requires that all Kentucky Wesleyan College administrative and business functions meet minimum requirements for security.

Commented [RS2]: Need to review, and finalize, approve and publish

5.3 Standards Implementation

Kentucky Wesleyan College has developed appropriate control standards, herein referred to as Information Security Standards, to support the Organization's Information Security policies. These standards are based on NIST Special Publication 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". The Information Security Standards define all Kentucky Wesleyan College directives for safeguarding information and ensuring that each organization complies with applicable laws, regulations, and commercial standards. Appropriate procedures have been documented that describe the tools, processes, and resources used to implement the Information Security Standards. The Kentucky Wesleyan College Information Security Standards are structured into eighteen (18) control groups.

Wherever appropriate, information security controls will comply with, reference, and implement the above standards. This position will be stated and reinforced in the security policy.

5.4 Regulatory and Security Best Practice Compliance

While not currently mapped to Kentucky Wesleyan College Information Security Standards, Kentucky Wesleyan College must also comply with the following:

- Electronic Communications Privacy Act (ECPA) - Federal law which specifies the standards by which law enforcement is permitted to access to electronic communications and associated data, affording important privacy protections to subscribers of emerging wireless and Internet technologies.
- U.S. Patriot Act - An antiterrorism law enacted by the U.S. Congress in October 2001, which gave certain additional new powers to the U.S. Department of Justice, the National Security Agency and other federal agencies for surveillance of electronic communications.
- Technology Education and Copyright Harmonization Act (TEACH) - Amendments to sections 110(2) and 112(f) of the U.S. Copyright Act., which was enacted to balance the perspectives of both copyright owners and content users for academic organizations.
- Executive Order 13224 - Federal Executive Order which provides a means to disrupt the financial support network for terrorists and terrorist organizations by authorizing the U.S. Government to designate and block the assets of foreign individuals.
- Higher Education Opportunity Act (HEOA) - Federal law which, among other requirements, addresses colleges and universities responsibilities relating to copyrighted materials.

It is the goal and intent of the WISP to ensure compliance with all known regulations and mandates as they are understood, and to make them an appropriate priority.

6. Risk Management

6.1 Set Goals and Objectives

Goals and objectives for Kentucky Wesleyan College's information security program will be established and corrective action plans (CAPs) will be documented and prioritized according to risk to the organization.

6.2 Identify Infrastructure

Kentucky Wesleyan College will identify all assets, systems, and networks critical to continued operation, as well as the dependencies between these essential resources. Effective risk management requires an understanding of the criticality of these resources to the organization.

6.3 Assess and Analyze Risks

Identifying risks is the single-most important step an organization can take to ensure the confidentiality, integrity, and availability of information assets. It is also an important component for achieving regulatory, commercial, and legal compliance.

Risk Reduction involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. The organization will implement security measures that reduce the risks to its information systems containing confidential information to reasonable and appropriate levels. Selection and implementation of such security measures will be based on a formal, documented risk management process.

6.4 Implement Risk Management Activities

The organization will manage risk on a continuous basis and implement necessary security measures to ensure the confidentiality, integrity, and availability of information systems containing confidential information. A risk assessment will be performed, at a minimum, annually. This involves identifying the risks to information assets and determining the probability of occurrence, the resulting impact, and additional safeguards to mitigate this impact. Strategies for managing risk should be commensurate with the risks to such systems. One or more of the following methods may be used to manage risk:

- Risk acceptance
- Risk avoidance
- Risk limitation
- Risk transference

The organization will manage the security state of organizational information systems and the environments in which those systems operate through the security authorization processes by:

- Kentucky Wesleyan College will be responsible for performing a risk assessment for all new services/capabilities/technologies being implemented before they can be implemented into production.

This position on risk management will be stated and reinforced in the security policy.

6.5 Measure Effectiveness

Kentucky Wesleyan College will regularly evaluate progress of security program implementation and risk management by reviewing and updating CAPs. Progress will be communicated to necessary stakeholders.

For detailed information regarding risk management, reference Kentucky Wesleyan College Risk Management procedure.

7. Computer and Technology Operations

7.1 General

Computer systems and networks, communications systems and other equipment belonging to or otherwise in the possession of Kentucky Wesleyan College are the property of Kentucky Wesleyan College and will be maintained solely by Kentucky Wesleyan College. These systems are provided for use in conducting Kentucky Wesleyan

College business, although reasonable personal use by workforce is permitted. Only Kentucky Wesleyan College owned assets will be used to process, store, or transmit Kentucky Wesleyan College owned data or information. The use of any Kentucky Wesleyan College system for commercial purposes other than that of Kentucky Wesleyan College is prohibited. There is no expectation of privacy when using any Kentucky Wesleyan College computers, systems, networks or other equipment and Kentucky Wesleyan College reserves the right to obtain access to any and all communications and data or information processed, stored, or transmitted by these systems at any time and without prior notice.

7.2 Network Security

Kentucky Wesleyan College network will be maintained in such a way that risk of corruption of data and unauthorized internal and external access is minimized. Vulnerabilities that arise in Kentucky Wesleyan College's network will be addressed according to Kentucky Wesleyan College's Vulnerability Management procedure. For more information on network security, reference Kentucky Wesleyan College Acceptable Use policy and Kentucky Wesleyan College Configurations.

7.3 Endpoint and Removable Media Protection

Commented [RS3]: ITS Policy Handbook

Controls will be implemented on Kentucky Wesleyan College laptops and removable media in order to protect the confidentiality and integrity of information contained therein.

- Kentucky Wesleyan College laptops and removable media will be encrypted.
- Kentucky Wesleyan College computing devices will be configured to time out and log out settings.
- End users will protect all Kentucky Wesleyan College owned computing devices and removable media.
- Virus detection and protection solutions will be implemented on Kentucky Wesleyan College owned computing devices.
- Kentucky Wesleyan College workforce will report any issues, including theft immediately to Information Technology.

For more information on endpoint and removable media protection, reference Kentucky Wesleyan College Acceptable Use Policy and Kentucky Wesleyan College Configurations.

7.4 User ID’s and Passwords

All workforce will be provided with a unique username and password to access any Kentucky Wesleyan College-owned system or application. Kentucky Wesleyan College workforce passwords will be required to meet minimum length, complexity, and reuse requirements in an attempt to protect confidential or sensitive data. All workforce will protect and not misuse user ID’s and passwords. For more information on user ID’s and passwords, reference Kentucky Wesleyan College Access Control procedure.

7.5 Access Rights

Only approved workforce will have access to Kentucky Wesleyan College systems and information and will be provided with the minimum level of access necessary to complete job duties. Network controls will be applied to prevent unauthorized network access. Any devices logged onto Kentucky Wesleyan College’s network will be configured to time out.

Remote access to Kentucky Wesleyan College’s environment will be granted only to those workforce with a legitimate documented business need.

Access to Kentucky Wesleyan College information, regardless of the form of information will only be performed for legitimate business purpose. No user is permitted to access, read, edit, print, copy, transfer or delete information maintained by any other user unless given permission by Human Resources upon account creation to do so. Access to systems owned or operated by Kentucky Wesleyan College’s third-party vendors is not permitted without proper authorization.

For more information on access rights, reference Kentucky Wesleyan College Access Control ITS Policy Handbook.

7.6 System Monitoring

At the discretion of the IT Team and Director of IT, Kentucky Wesleyan College reserves the right to monitor or review activity on any organization-owned system and without notice. Banners explaining Kentucky Wesleyan College's position on system monitoring will be implemented on all assets where logins happen. For more information on system monitoring, reference Kentucky Wesleyan College's Help Desk system.

7.7 Data Classification and Handling

Kentucky Wesleyan College workforce will classify and label all information and data. Kentucky Wesleyan College workforce will make all efforts to redact any information classified as confidential or sensitive when appropriate to do so. Kentucky Wesleyan College data and information will be retained according to applicable local and federal guidelines. All Kentucky Wesleyan College data and information will be destroyed when no longer needed. Kentucky Wesleyan College workforce will be responsible for appropriately processing, storing, and transmitting Kentucky Wesleyan College information or data. For more information on data classification and handling, reference Kentucky Wesleyan College Data Classification and Handling and Kentucky Wesleyan College Data and Information Destruction ITS Policy Handbook.

7.8 Acceptable Use

All workforce will appropriately use Kentucky Wesleyan College computer systems and networks, communications systems and other equipment belonging to Kentucky Wesleyan College, and in such a way that does not violate any law or regulation. Examples include, but are not limited to:

- Voicemail
- Software
- Email
- Internet

For more information on acceptable use, reference Kentucky Wesleyan College's Acceptable Use policy.

7.9 Personnel Security

All Kentucky Wesleyan College workforce will be provided with all relevant and necessary policies, standards, and procedures necessary to perform job duties upon hire and annually. Kentucky Wesleyan College workforce will be provided with relevant training on these topics and will be expected to attest to having read and understood all materials provided. Kentucky Wesleyan College will assign a risk designation to each position and screen, transfer and terminate workforce appropriately. For more information on personnel security, reference Kentucky Wesleyan College Personnel Security procedure.

Commented [RS4]: No defined in ITS Policy Handbook

7.10Vendor Management

Kentucky Wesleyan College enters into contracts with third-party vendors for essential services. Kentucky Wesleyan College will conduct reasonable due diligence on vendors. Kentucky Wesleyan College will ensure all reasonable and appropriate agreements are in place to protect any Kentucky Wesleyan College data or information processed, stored, or transmitted by third-party vendors. For more information on vendor management, reference Kentucky Wesleyan College Vendor Management ITS Policy Handbook.

8. Exception Process

Compliance with the Kentucky Wesleyan College WISP, along with related policies, standards and procedures are necessary to ensure the confidentiality, integrity, and availability of organizational information assets. Kentucky Wesleyan College leadership recognizes, however, that full compliance with the WISP may not be possible, due to operational constraints. Non-compliance with any organization standard will be documented as an exception, reviewed, approved, and addressed. Documented exceptions will include:

- The standard where non-compliance may exist;
- The specific non-compliant situation, service, or process;
- The operational risk introduced by the gap;
- Any current controls which may partially mitigate the risk;

- If the decision is to remediate the gap, a corrective action plan (CAP) must be developed and assigned to an owner;
- The acceptance of the risk and remediation plans.

9. Information Security Road Map

9.1 Overview

The Information Security Roadmap describes the current and planned security priorities of the organization. For more information regarding current and planned security priorities, reference Kentucky Wesleyan College Security Roadmap.

10. Related Documentation

10.1 Written Information Security Program (WISP)

Regulation

Compliance Checklist

11. Plan Authority

This Plan is issued by the Director of Information Technology for Kentucky Wesleyan College.

12. Revision History

Version	Date	Author	Revisions
1.0		GreyCastle Security	Initial Draft
1.1			

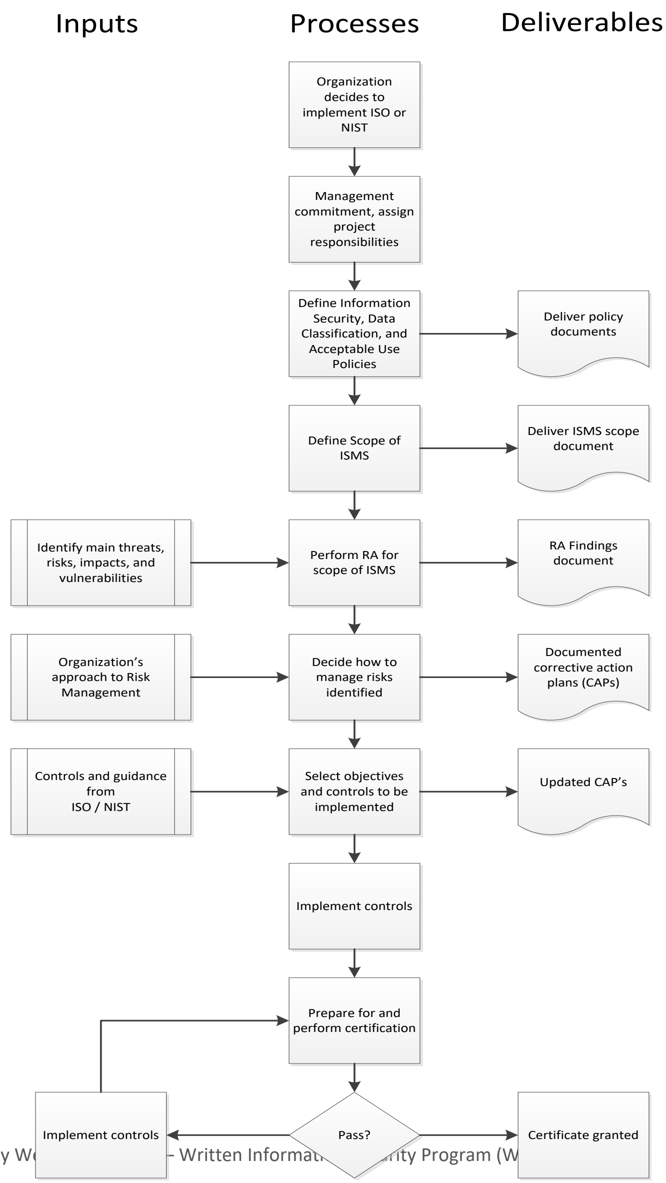
13. Approvals

Executive	Director of Information Technology
Name	Name
Title	Title
Date	Date
Signature	Signature

14. APPENDIX A – Process Overview

Commented [RS5]: Review process

The diagram below is an overview that depicts the flow and scope of the WISP program:


Inputs
Processes
Deliverables
Organization decides to implement ISO or NIST
Management commitment, assign project responsibilities
Define Information Security, Data Classification, and Acceptable Use Policies
Deliver policy documents
Define Scope of ISMS
Deliver ISMS scope document
Identify main threats, risks, impacts, and vulnerabilities
Perform RA for scope of ISMS
RA Findings document
Organization's approach to Risk Management
Decide how to manage risks identified
Documented corrective action plans (CAPs)
Controls and guidance from ISO / NIST
Select objectives and controls to be implemented
Updated CAP's
Implement controls
Prepare for and perform certification
Implement controls
Pass?
Certificate granted