




Procedure: Information Security Governance Plan	
Issue Date: 1/1/2023	Procedure Number: Planning - 05
Revision Number: 1.0	NIST Control: PM-1
Revision Date: 1/1/2023	Owner: Director of Information Technology


Contents

- 1. Definitions..... 1
- 2. Purpose..... 2
- 3. Mission..... 2
- 4. Roles and Responsibilities..... 2
 - 1.1 Executive Committee Responsibilities 2
 - 1.2 Information Security Steering Committee Responsibilities 3
 - 1.3 Information Security Officer (ISO) 4
 - 1.3.1 Measurement and Effectiveness, including: 4
 - 1.4 End User Responsibilities..... 4
- 5. Revisions 5
- Appendix A – Committee Members 5

	AWARENESS PROGRAM PLAN
Effective Date 1/1/2023	Version 1.0

1. Definitions

Term	Meaning
<i>Written Information Security Program - WISP</i>	A document detailing a description of the complete manner in which a company implements the administrative, technical, or physical safeguards in place to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle member information.
<i>Executive Committee</i>	A management committee tasked with upholding the Board's interests in a particular subject area. Such a committee is normally populated with senior executives of the corporation. Focus of the Executive Committee in the context of this Plan is to ensure that strategic direction and resourcing is set for information security, in alignment with the corporate goals and objectives.
<i>Information Security Steering Committee</i>	A cross-functional committee that is associated with the tactical management of the information security objectives handed down by the Executive Committee.
<i>Information Security Policy</i>	The document or documents that specify the corporate policy with respect to information security.
<i>Acceptable Use Policy</i>	A policy that specifies the responsibility of any employee or contractor that receives access to the corporation's data and data processing equipment, including computers, network, systems, and data.
<i>Information Security Governance Plan</i>	This document. A formal description of the charter for the Information Security Steering Committee and an explanation of the roles and responsibilities for the committees involved in the governance and continuous improvement of the company's information security program.

	<p><i>AWARENESS PROGRAM PLAN</i></p>
<p>Effective Date 1/1/2023</p>	<p>Version 1.0</p>

2. Purpose

The purpose of this Information Security Governance Plan is to set the direction of governance of Kentucky Wesleyan College’s Information Security Program through a risk-based approach. Roles and responsibilities will be established to ensure the maintenance and a continual improvement of Kentucky Wesleyan College’s Information Security Program. Operating areas will implement documented controls and ensure compliance with the Information Security Program.

3. Mission

The mission of Kentucky Wesleyan College’s Information Security Program is to preserve the confidentiality, integrity, and availability of Kentucky Wesleyan College information assets, in accordance with the Information Security Policy. The Information Security Program serves as the organization’s mechanism to appropriately identify, select, maintain, and improve information security controls.


The protection of information assets owned or managed by Kentucky Wesleyan College is not the sole responsibility of the Information Security Program. In order to create a holistic and secure environment, multiple programs must work together within clearly defined responsibilities.

4. Roles and Responsibilities

1.1 Executive Committee Responsibilities

The Executive Committee is the strategic governance body that sets the direction of the information security objectives, provides oversight of the information security progress, and is ultimately responsible to the Board of Directors for the overall health of the Information Security program. The Executive Committee:

- Consistently demonstrates support and commitment to the Information Security Program, its objectives, goals, and enforcement.

	<p><i>AWARENESS PROGRAM PLAN</i></p>
<p>Effective Date 1/1/2023</p>	<p>Version 1.0</p>


- Ensures the Information Security Program’s continuing adequacy, effectiveness, and efficiency.
- Responsible for the final determination of risk acceptance or mitigation, should there be conflict of opinions between the Information Security Program, the Information Security Steering Committee and/or the Operating areas.

1.2 Information Security Steering Committee Responsibilities

The Information Security Steering Committee is a cross-functional, management committee. The responsibilities of the Information Security Steering Committee are as follows:

1. Report the status and direction of the Information Security Program to the Executive Committee.
2. Review and recommend strategies related to the Information Security Program.
3. Review and approve information security policies and standards, and other supporting documentation.
4. Approve and maintain oversight of the risk management process, including risk assessment methodology, risk acceptance criteria, residual and accepted risks;
5. Review the Business Impact Analysis (BIA) and the Business Continuity Plan;
6. Perform a full review of the Written Information Security Program (WISP);
7. Approve actions to resolve issues identified during reviews in an effective and timely manner;
8. Advise on year-over-year goals and priorities for the Information Security Program.
9. Ensure compliance with all Information Security Program requirements, policies, standards, and procedures; and
10. Review findings results from various audits and assessments
11. Oversee implementation of remediation plans to ensure high priority risks have been resolved.

Additional detail on the operation, responsibilities and membership of the Steering Committee may be found in the Steering Committee Charter later in this document.

	<p><i>AWARENESS PROGRAM PLAN</i></p>
<p>Effective Date 1/1/2023</p>	<p>Version 1.0</p>

1.3 Information Security Officer (ISO)

Kentucky Wesleyan College maintains a contractual relationship with GreyCastle Security to provide a virtual Chief Information Security Officer (vCISO) services. For legal and accountability objectives, the Information Security Program is led by the Director of Information Technology for Kentucky Wesleyan College, while leveraging the vCISO relationship. The Information Security Program is governed by the Information Security Steering Committee.


To establish and maintain the Information Security Program, the ISO will assure that the following responsibilities are carried out:

1.3.1 *Measurement and Effectiveness, including:*

1. Vulnerability management.
2. Security incident management team leadership.
3. As requested, provide consulting services to operating areas.
4. Establish physical security parameters.
5. Change Management

1.4 End User Responsibilities

1. Understand and conform with the Acceptable Use Policy and all other applicable policies, standards, procedures, and guidance instructions.
2. Protect and properly use all company assets made available to the End User; and
3. Immediately communicate any detected security incident or anomaly through the respective channels and in accordance with the internal policies and procedures.

	<p><i>AWARENESS PROGRAM PLAN</i></p>
<p>Effective Date 1/1/2023</p>	<p>Version 1.0</p>

5. Revisions

Version	Date	Author	Revisions
1.0		GreyCastle Security	Initial Draft
1.1			

Appendix A – Committee Members

- Name, Title, Department
- Name, Title, Department