Procedure: Information Security Policy	
Issue Date: 5/1/2022	**Revision Date: 1/1/2023**
Revision Number: 1.1	**NIST Control: AT**
Owner: Director of Information Technology	

Contents

THE Wesleyan Way KENTUCKY WESLEYAN COLLEGE	*Information Security Policy*
Effective Date 1/1/2023	Version 1.0

1. Introduction

The purpose of this policy is to assist the organization in its efforts to fulfill its fiduciary responsibilities relating to the protection of information assets and comply with regulatory and contractual requirements involving information security and privacy. This policy framework consists of eighteen (18) separate policy statements, with supporting Standards documents, based on guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-171.

Although no set of policies can address every possible scenario, this framework, taken as a whole, provides a comprehensive governance structure that addresses key controls in all known areas needed to provide for the confidentiality, integrity and availability of the organization's information assets. This framework also provides administrators guidance necessary for making prioritized decisions, as well as justification for implementing organizational change.

2. Purpose

The purpose of this Information Security Policy is to clearly establish Kentucky Wesleyan College role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives enables Kentucky Wesleyan College to implement a comprehensive system-wide Information Security Program.

3. Scope

The scope of this policy includes all information assets governed by the organization. All personnel and service providers who have access to or utilize assets of the organization, including data at rest, in transit or in process shall be subject to these requirements. This policy applies to:

- All information assets and IT resources operated by the organization;

- All information assets and IT resources provided by the organization through contracts, subject to the provisions and restrictions of the contracts; and
- All authenticated users of Kentucky Wesleyan College information assets and IT resources.

4. Implementation

Kentucky Wesleyan College needs to protect the availability, integrity and confidentiality of data while providing information resources to fulfill the organization's mission. The Information Security Program must be risk-based and implementation decisions must be made based on addressing the highest risk first.

Kentucky Wesleyan College's administration recognizes that fully implementing all controls within the NIST Standards is not possible due to organizational limitations and resource constraints. Administration must implement the NIST standards whenever possible, and document exceptions in situations where doing so is not practicable.

5. Roles and Responsibilities

Kentucky Wesleyan College has assigned the following roles and responsibilities:

1) The Director of Information Technology also serves as the Chief Information Officer: The Director of Information Technology is accountable for the implementation of the Information Security Program including:

    a) Security policies, standards, and procedures

    b) Security compliance including managerial, administrative and technical controls

    The Chief Information Officer is to be informed of information security implementations and ongoing development of the Information Security Program design.

2) Information Security Committee: The group is responsible for the design, implementation, operations and compliance functions of the Information Security Program for all Kentucky Wesleyan College constituent units. The committee is comprised of senior staff and functions as the Information Security Program Office.

3) Information Security Officer: GreyCastle Security is supportive and performs as the Information Security Officer for Kentucky Wesleyan College. The Director of Information Technology alongside GreyCastle are responsible for the development, implementation and maintenance of a comprehensive Information Security Program for Kentucky Wesleyan College. This includes security policies, standards and procedures which reflect best practices in information security.

6. Information and System Classification

Kentucky Wesleyan College must establish and maintain security categories for both information and information systems. For more information, reference the Data Classification Policy.

7. Provisions for Information Security Standards

The Kentucky Wesleyan College Security Program is framed on National Institute of Standards and Technology (NIST) and controls implemented based on the Center for Internet Security (CIS) Critical Security Controls priorities. Kentucky Wesleyan College must develop appropriate control standards and procedures required to support the organization's Information Security Policy. This policy is further defined by control standards, procedures, control metrics and control tests to assure functional verification.

The Kentucky Wesleyan College Security Program is based on NIST Special Publication 800-171. This publication is structured into 18 control groupings, herein referred to as

Information Security Standards. These Standards must meet all statutory and contractual requirements.

i. Access Control (AC)

Kentucky Wesleyan College must limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

ii. Awareness and Training (AT)

Kentucky Wesleyan College must: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of organization information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

iii. Audit and Accountability (AU)

Kentucky Wesleyan College must: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

iv. Assessment and Authorization (CA)

Kentucky Wesleyan College must: (i) periodically assess the security controls in organization information systems to determine if the controls are effective in their

application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organization information systems; (iii) authorize the operation of the organization's information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

v. Configuration Management (CM)

Kentucky Wesleyan College must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

vi. Contingency Planning (CP)

Kentucky Wesleyan College must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the organization's information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

vii. Identification and Authentication (IA)

Kentucky Wesleyan College must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Kentucky Wesleyan College information systems.

viii. Incident Response (IR)

Kentucky Wesleyan College must: (i) establish an operational incident handling capability for organization information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organization officials and/or authorities.

ix. Maintenance (MA)

Kentucky Wesleyan College must: (i) perform periodic and timely maintenance on organization information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

x. Media Protection (MP)

Kentucky Wesleyan College must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) encryption, where applicable, (iiii) sanitize or destroy information system media before disposal or release for reuse.

xi. Physical and Environmental Protection (PE)

Kentucky Wesleyan College must: (i) limit physical access to information systems, equipment and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

xii. Planning (PL)

Kentucky Wesleyan College must develop, document, periodically update and implement security plans for organization information systems that describe the security controls in place or planned for the information systems as well as rules of behavior for individuals accessing the information systems.

xiii. Personnel Security (PS)

Kentucky Wesleyan College must: (i) ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions; (ii) ensure that organization information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with Kentucky Wesleyan College security policies and procedures.

xiv. Risk Assessment (RA)

Kentucky Wesleyan College must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage or transmission of organizational information.

xv. System and Services Acquisition (SA)

Kentucky Wesleyan College must: (i) allocate sufficient resources to adequately protect organization information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third- party providers employ adequate security measures, through federal and state law and

contract, to protect information, applications and/or services outsourced from the organization.

xvi. System and Communications Protection (SC)

Kentucky Wesleyan College must: (i) monitor, control and protect organization communications (i.e., information transmitted or received by organization information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within organization information systems.

xvii. System and Information Integrity (SI)

Kentucky Wesleyan College must: (i) identify, report and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organization information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

xviii. Program management (PM)

Kentucky Wesleyan College must implement security program management controls to provide a foundation for the organizational Information Security Program.

8. Enforcement

Kentucky Wesleyan College may temporarily suspend or block access to any individual or device when it appears necessary to do so in order to protect the integrity, security or functionality of organization and computer resources.

Any personnel found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

9. Privacy

Kentucky Wesleyan College must make every reasonable effort to respect a user's privacy. However, personnel do not acquire a right of privacy for communications transmitted or stored on organization resources.

Additionally, in response to a judicial order or any other action required by law or permitted by official organization policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the organization, the Chief Information Officer, or an authorized agent, may access, review, monitor and/or disclose computer files associated with an individual's account.

10. Exceptions

Exceptions to the policy may be granted by the Director of Information Technology, or his or her designee. To request an exception, submit an Information Security Exception request to Information Technology Department.

11. Disclaimer

Kentucky Wesleyan College disclaims any responsibility for and does not warrant information and materials residing on non-Kentucky Wesleyan College systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of Kentucky Wesleyan College.

12. References

- NIST SP 800-171
- The Gramm - Leach Bliley Act (GLBA)

- Family Educational Rights and Privacy Act (FERPA)
- State of Kentucky Cybersecurity Bill (KRS 61.932(1)(b))
- FIPS-199

13. Related Policies

- Kentucky Wesleyan College Data Classification Policy
- Data Classification Procedure
- Acceptable Use Policy

14. Responsible Department

Information Technology

15. Policy Authority

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

16. Revision History

Version	Date	Author	Revisions
1.0		GreyCastle Security	Initial Draft
1.1	6-15-2022	Kentucky Wesleyan Team	Review/Approval

17. Approvals

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