OHIO CHRISTIAN
UNIVERSITY

Information Technology

1476 Lancaster Pike
Circleville, OH 43113
it.ohiochristian.edu
blazertech@ohiochristian.edu
740-420-5907

DOCUMENT #:POL-0001
EFFECTIVE: XX-XXX-2021
OWNER: ISO

INFORMATION SECURITY

CONTENTS

1.0 INTRODUCTION

The purpose of this policy is to assist the university in its efforts to fulfill its fiduciary responsibilities relating to the protection of information assets and to 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 800-171r2.

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 university's information assets. This framework also provides administrators the guidance necessary for making prioritized decisions as well as justification for implementing organizational change.

2.0 PURPOSE

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

3.0 SCOPE

The scope of this policy includes all information assets governed by the university. All personnel and service providers who have access to or utilize assets of the university, 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 university
- All information assets and IT resources provided by the university through contracts subject to the provisions and restrictions of the contracts
- All authenticated users of Ohio Christian University information assets and IT resources.

4.0 IMPLEMENTATION

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

Ohio Christian University'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.

5.0 ROLES AND RESPONSIBILITIES

Ohio Christian University has assigned the following roles and responsibilities:

1) Executive Director of Information Technology: The Executive 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 Executive Director of Information Technology 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 Ohio Christian University 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 Ohio Christian University. GreyCastle is responsible for the development, implementation, and maintenance of a comprehensive Information Security Program for Ohio Christian University. This includes security policies, standards, and procedures which reflect best practices in information security.

6.0 INFORMATION AND SYSTEM CLASSIFICATION

Ohio Christian University must establish and maintain security categories for both information and information systems. For more information, reference the Data Classification Policy.

7.0 PROVISIONS FOR INFORMATION SECURITY STANDARDS

The Ohio Christian University Security Program is framed on National Institute of Standards and Technology (NIST) and controls implemented based on SANS Critical Security Controls priorities. Ohio Christian University must develop appropriate control standards and procedures required to support the university's Information Security Policy. This policy is further defined by control standards, procedures, control metrics, and control tests to assure functional verification.

The Ohio Christian University Security Program is based on NIST Special Publication 800-171r2. This publication is structured into 17 control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements.

7.1 ACCESS CONTROL (AC)

Ohio Christian University must limit information system access to authorized users, to 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.

7.2 AWARENESS AND TRAINING (AT)

Ohio Christian University must:

- 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 the university's information systems; and
- Ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

7.3 AUDIT AND ACCOUNTABILITY (AU)

Ohio Christian University must:

- 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 restricted data and restricted networks, at a minimum
- Ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

7.4 ASSESSMENT AND AUTHORIZATION (CA)

Ohio Christian University must:

- Periodically assess the security controls in university information systems to determine if the controls are effective in their application
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in university information systems
- Authorize the operation of the university's information systems and any associated information system connections
- Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

7.5 CONFIGURATION MANAGEMENT (CM)

Ohio Christian University must:

- Establish and maintain baseline configurations and inventories of university information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles
- Establish and enforce security configuration settings for information technology products employed in university information systems.

7.6 CONTINGENCY PLANNING (CP)

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

7.7 IDENTIFICATION AND AUTHENTICATION (IA)

Ohio Christian University 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 university information systems.

7.8 INCIDENT RESPONSE (IR)

Ohio Christian University must:

- Establish an operational incident handling capability for university information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities
- Track, document, and report incidents to appropriate university officials and/or authorities.

7.9 MAINTENANCE (MA)

Ohio Christian University must:

- Perform periodic and timely maintenance on university information systems
- Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

7.10 MEDIA PROTECTION (MP)

Ohio Christian University must:

- Protect information system media, both paper and digital
- Limit access to information-on-information system media to authorized users
- Utilize encryption, where applicable
- Sanitize or destroy information system media before disposal or release for reuse

7.11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

Ohio Christian University must:

- Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals
- Protect the physical plant and support infrastructure for information systems
- Provide supporting utilities for information systems
- Protect information systems against environmental hazards
- Provide appropriate environmental controls in facilities containing information systems.

7.12 PLANNING (PL)

Ohio Christian University must develop, document, periodically update, and implement security plans for university 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.

7.13 PERSONNEL SECURITY (PS)

Ohio Christian University must:

- Ensure that individuals occupying positions of responsibility within the university are trustworthy and meet established security criteria for those positions
- Ensure that university information and information systems are protected during and after personnel actions such as terminations and transfers
- Employ formal sanctions for personnel failing to comply with university security policies and procedures

7.14 RISK ASSESSMENT (RA)

Ohio Christian University must periodically assess the risk to university operations (including mission, functions, image, or reputation), university assets, and individuals resulting from the operation of university information systems and the associated processing, storage, or transmission of university information.

7.15 SYSTEM AND SERVICES ACQUISITION (SA)

Ohio Christian University must:

- Allocate sufficient resources to adequately protect university information systems
- Employ system development life cycle processes that incorporate information security considerations
- Employ software usage and installation restrictions
- Ensure that third- party providers employ adequate security measures, through federal and state law, and through contract, to protect information, applications, and/or services outsourced from the university.

7.16 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Ohio Christian University must:

- Monitor, control, and protect university communications (i.e., information transmitted or received by university information systems) at the external boundaries and key internal boundaries of the information systems for restricted data transmissions
- Employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within university information systems.

7.17 SYSTEM AND INFORMATION INTEGRITY (SI)

Ohio Christian University must:

- Identify, report and correct information and information system flaws in a timely manner
- Provide protection from malicious code at appropriate locations within university information systems
- Monitor information system security alerts and advisories and take appropriate actions in response

7.18 PROGRAM MANAGEMENT (PM)

Ohio Christian University must implement security program management controls to provide a foundation for the university Information Security Program.

8.0 ENFORCEMENT

Ohio Christian University 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 university and computer resources.

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

9.0 PRIVACY

Ohio Christian University workforce members maintain no expectation of privacy while accessing, utilizing, transmitting, or storing information or communications on OCU systems [See employee handbook].

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

10.0 EXCEPTIONS

Exceptions to the policy may be granted by the Executive Director of Information Technology, or his or her designee. To request an exception, submit an Information Security Exception request to the IT Helpdesk at blazertech@ohiochristian.edu.

11.0 DISCLAIMER

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

12.0 REFERENCES

- NIST SP 800-171,
- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- FIPS-199
- 13.0 Related Policies
- Ohio Christian University Data Classification Policy
- Data Classification Procedure
- Acceptable Use Policy

14.0 RESPONSIBLE DEPARTMENT

Information Systems

15.0 POLICY AUTHORITY

This policy is issued by Human Resources for Ohio Christian University

16.0 REVISION HISTORY

Version	Date	Author	Revisions
1.0		Information Technology	Initial Draft

17.0 APPROVALS

Executive	Chief Security Officer
Ted Perry	Amber Smith
CFO/COO	Executive Director of Information Technology
Date	Date
Signature	Signature