POLICY #3358-7-21
Section: Information Technology
Original Policy: N/A
Revision Approved: 06/24/2026
Approved by: Board of Trustees

CYBERSECURITY PROGRAM CHARTER

PURPOSE

The Cybersecurity Program (Program) establishes Edison State Community College's enterprise-wide governance framework to manage cybersecurity risk in a manner commensurate with institutional size, complexity, resources, and risk tolerance. The Program supports the confidentiality, integrity, and availability of institutional information and technology resources necessary to sustain instruction, student services, and business operations. The Program adopts the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 as its guiding model for governance, risk prioritization, and continuous improvement, using the Functions: Govern, Identify, Protect, Detect, Respond, and Recover.

POLICY STATEMENT

The Program establishes intent and accountability at the institutional level. Specific safeguards, controls, and technologies are implemented through separate policies, standards, procedures, risk assessments, and phased implementation plans based on institutional priorities and available resources.

By adoption of this Charter, the Board of Trustees delegates authority to the President, with further delegation to the Chief Information Officer (CIO), to administer and oversee the Cybersecurity Program. This includes establishing policies and standards, approving risk-based exceptions, coordinating compliance activities, and allocating resources consistent with institutional priorities. The Program constitutes the College's recognized cybersecurity program for purposes of Ohio's cybersecurity safe harbor statutes and is based on an industry-recognized framework (NIST CSF 2.0).

Alignment with Institutional Mission, Vision, Values, and Strategic Plan

The Cybersecurity Program supports the College's mission by protecting the digital systems and information essential to learning, student success, workforce development, and community engagement. Cyber resilience and data protection are foundational to institutional trust, continuity, and stewardship of public resources. Cybersecurity governance is integrated into strategic planning, risk management, and performance assessment rather than treated as a standalone technical function.

Program reporting and risk discussions are aligned with established institutional governance forums and strategic review cycles. Communications focus on risk, impact, and readiness rather than technical detail.

Scope

The Cybersecurity Program applies institution-wide and encompasses people, information, systems, and third-party relationships to the extent they create institutional cyber risk. It applies to all College-owned or managed information systems, cloud services, and data regardless of format.

While all institutional data is in scope, control requirements are determined through data classification, regulatory applicability, and risk assessments. Not all systems or data require identical safeguards, and controls are implemented proportionate to risk, sensitivity, and operational impact.

Governance Structure

Board of Trustees. The Board provides oversight of institutional cybersecurity risk, approves this Charter and related risk tolerance statements, and receives periodic high-level reporting regarding risk posture, significant incidents, and program maturity. The Board's role is strategic and fiduciary rather than operational.

President. The President is accountable for ensuring cybersecurity risk is managed as an institutional risk and integrated into budgeting, planning, and executive decision-making.

Chief Information Officer. The CIO serves as Program Executive responsible for administering the Cybersecurity Program, coordinating cross-functional participation, issuing standards, approving risk exceptions, and reporting to executive leadership and the Board. Where required under applicable regulations, the CIO serves as or designates a Qualified Individual.

Shared Governance. Cybersecurity and data protection are shared institutional responsibilities. Administrative leadership, academic leadership, and data owners are accountable for complying with policies, participating in risk management, and supporting controls within their areas.

Legal and Regulatory Alignment

The Program aligns with applicable federal, state, and contractual requirements in a risk-based manner. Key obligations include Ohio cybersecurity statutes and reporting requirements, FERPA, GLBA Safeguards Rule obligations associated with Title IV participation, limited PCI DSS obligations for payment processing, and HIPAA requirements where legally applicable outside FERPA-covered records. Applicability determinations and control implementation are documented and periodically reviewed.

Responsibility for compliance with these obligations is institutional and executive in nature. Technology controls support compliance but do not transfer accountability away from institutional leadership or data owners.

Program Domains

The Cybersecurity Program includes governance and oversight of the following domains, implemented through phased and risk-prioritized execution plans:

- Risk management and cybersecurity governance
- Asset and data inventory appropriate to institutional capacity
- Identity and access management safeguards
- Data protection and privacy governance
- Security monitoring and incident response capabilities, delivered internally or through managed services as determined by risk
- Business continuity and disaster recovery planning for critical operations
- Third-party and supply-chain risk management commensurate with exposure
- Security awareness and role-based training

Descriptions of these domains establish oversight intent. Detailed control requirements are maintained in subordinate policies and standards and adjusted based on maturity, funding, and institutional risk tolerance.

Reporting, Metrics, and Accountability

Management provides periodic, board-appropriate reporting focusing on risk posture, material changes, significant incidents, and progress toward target maturity. Metrics emphasize trends, coverage, and risk reduction rather than technical detail. Benchmarking against NIST CSF Profiles supports transparency without implying full implementation of every framework element.

Continuous Improvement

The Cybersecurity Program follows a continuous improvement model. Risk assessments, maturity evaluations, and roadmap updates occur on a recurring basis, with priorities adjusted to reflect emerging threats, regulatory changes, institutional initiatives, and available resources. Improvements are phased and sustainable rather than speculative or aspirational.

Charter Review and Amendment

This Charter is reviewed at least annually or upon significant changes in regulatory expectations or institutional risk posture. Amendments are proposed by the President upon recommendation of the CIO and require Board approval. Upon adoption, this Charter supersedes conflicting prior directives.

PERSONS AFFECTED

All trustees, employees, students, contractors, volunteers, and third parties with access to college systems or data.

DEFINITIONS

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)
The National Institute of Standards and Technology (NIST) is a United States Department of Commerce agency whose mission is to promote American innovation and industrial competitiveness. As a part of that mission, they provide guidance on a wide range of topics including cybersecurity.

CYBERSECURITY FRAMEWORK (CSF) 2.0
A widely recognized industry standard cybersecurity framework that provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization regardless of its size, sector, or maturity to better understand, assess, prioritize, and communicate its cybersecurity efforts.