9.1 INFORMATION SECURITY PROGRAM POLICY

Original Date of Issue: 5/20/2026

1. Purpose

This Information Security Program Policy ("Policy") lays out the governance and risk management framework for Delaware County Community College ("DCCC") Information Technology ("IT") systems and environments. Maintaining a secure information environment is a DCCC strategic objective. DCCC Administration demonstrates its commitment to information and cyber security through the maintenance of an Information Security Program ("ISP"), this Policy, and associated policies and procedures. This Policy and other relevant policies shall be available to all Authorized Users as a reference for information security obligations.

2. Scope

This Policy applies to all authorized users who are provided access to DCCC systems and environments. It defines the access and account management requirements for all DCCC-controlled information assets. The DCCC environment is comprised of DCCC-controlled domains and platforms used to facilitate DCCC processes under DCCC control.

3. Definitions

See Glossary (https://catalog.dccc.edu/policies-procedures/administrative-computing/).

4. Roles and Responsibilities

Accountable

Vice President ("VP") of Finance and Administration: The VP of Finance and Administration is ultimately accountable for the maintenance of this Policy and the establishment of implementing procedures but may delegate implementation of this Policy to the AVP of IT (defined below).

Responsible

Vice President of Information Technology ("VP of IT"): The VP of IT is responsible for the day-to-day operation of this Policy and implementing procedures. The AVP of IT will also be designated as the Qualified Individual as required under 16 C.F.R. 314.4 (https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4)(a).

The VP of IT or the VP of Finance and Administration must report in writing to the DCCC Board of Trustees at least annually with an overall assessment of DCCC's compliance with its information security program and material information pertaining to the program including risk assessments, risk management and control decisions, service provider arrangements, test results, security events and how DCCC responded to such events, as well as recommendations for changes in the information security program.

Supportive

IT Team: The IT Team is responsible for identifying risks in the information system in accordance with this Policy and its implementing procedures.

Legal: Legal is responsible for identifying applicable legal, regulatory, and contractual obligations for risk assessment.

Asset Owners: Asset Owners are responsible for identifying risks with regard to their assets.

Data Owners: Data Owners are responsible for identifying risks with regard to their data.

Consulted

Managers: Managers are consulted in the establishment of this Policy and its implementing procedures.

Informed

All Authorized Users: All Authorized Users shall be informed of and acknowledge this Policy.

5. Information Security Programs

Information security is an essential part of DCCC's strategic objective. In addition to ensuring the confidentiality, availability, and integrity of DCCC information, it imbues confidence in clients, stakeholders, and partners that its information is secure in DCCC's care. An information security program integrates all operational, legal, and regulatory requirements into a single set of controls such that they are part of a comprehensive program.

Structure

Information security policies will define the high-level requirements and controls that govern behavior with regard to information security for all Authorized Users, systems, and assets. The topics are as follows:

- 9.1 Information Security Policy
- 9.2 Acceptable Use Policy
- 9.4 Access and Account Management
- 9.5 Network Management
- 9.6 Vulnerability and Patch Management
- 9.7 Incident Response and Business Continuity
- 9.8 Secure Configuration and Change Management
- 9.9 Asset and Data Management
- 9.10 Centralized Logging and Monitoring
- 9.11 Encryption and Key Management
- 9.12 Third Party and Vendor Management
- 9.13 Secure Code Development

These policies shall be reviewed as deemed necessary by the VP of IT in light of: (a) the results of DCCC's system monitoring and testing; (b) DCCC's risk assessment results; or (c) periodically as needed to address external and internal changes that may have a material impact on DCCC's security program, operations, or business arrangements. Processes, procedures, and, where required, plans, may be documented to implement policy. Policies must be reviewed and approved by the Board of Trustees, whereas processes, procedures, and plans can be reviewed and approved by the owner of the policy that such document is subordinate to.

Exceptions

While the information security policies should be followed in the normal course, sometimes an exception is necessary. To request an exception, the requestor must submit a request via the ticketing system with a business justification. The VP of IT shall review the exception, analyze the risk, document the same in the ticket, provide a recommendation,

and identify any necessary compensating controls. The VP of IT shall review the risk assessment, approve or deny the exception, or request additional information. Approved exceptions shall be documented in the risk register and reviewed periodically as deemed necessary by the VP of IT. Where necessary, compensating controls shall be implemented and documented to mitigate risk from the exception.

6. Risk Management

DCCC adopts a cyclical preparation, risk identification, risk analysis, risk evaluation, and risk treatment framework. Organizational risk decisions shall be communicated via established channels, including integration into information security policies, processes, procedures, and documentation. The VP of IT shall conduct a periodic risk assessment and internal audit of security controls at the direction of the Administration.

Identification

The VP of IT shall begin the risk management process by consulting with the VP of Finance and Administration to ascertain the organizational strategy ("Objectives"), internal and external stakeholder needs, and risk appetite and tolerance with respect to each therein. Before completing the risk assessment, the VP of IT shall review, and if deemed necessary by the VP of IT, revise its IT asset inventory. The VP of IT shall also obtain an estimation of budgetary availability for treatment or risk in each strategic sector. In the Identification phase, the risks across business units shall be identified on the organizational; mission and business; legal, regulatory, and contractual requirements; cyber supply chain risk; and information system levels. Additionally, the VP of IT shall ensure they understand system critical objectives, capabilities, services, and dependencies.

DCCC shall maintain a written risk register to track its identified risks, associated analysis, and chosen response. It shall also keep a Plan of Action and Milestones ("POAM") to track identified non-compliance with controls with accountable milestones to close compliance gaps. DCCC shall perform a risk assessment periodically as deemed necessary by the VP of IT in light of changes to DCCC's operations and the emergence of new threats to DCCC Sensitive and Confidential Information, including personally identifiable information protected under applicable data protection laws.

Analysis and Evaluation

The risk assessment shall include a description of: (a) the criteria used to identify security risks and threats; (b) how current systems are assessed in the context of identified risks and threats; and (c) how identified risks will be mitigated or accepted, including how the DCCC will address such risks.

DCCC shall analyze risks using the following formula:

Risk = Likelihood * Impact

Likelihoods and impacts shall be given definitions. The VP of Finance and Administration may develop a procedure for evaluating each risk based on the analysis of the risk and the risk tolerance for each risk identified in the preparation phase.

Treatment

The evaluation shall result in a treatment plan based on one of the following actions: reduction, avoiding, sharing/transfer, or accepting. Strategic opportunities shall be evaluated alongside the risks. All actions shall be documented in the risk register, POAM tracker, and relevant information security program documents. Decisions on risk shall be properly communicated to relevant internal and external stakeholders.

Audit and Periodic Review

The Administration is committed to improving its information security system. It ensures that sufficient resources are allocated to the information security program including budget considerations, staffing, and review.

The Administration shall review the results of each, with the risk assessment determining whether the security controls must be altered to fit organizational strategy, requirements, and mission, along with an internal audit determining whether control implementation is adequate. Improvements shall be identified, documented, and implemented based on these assessments.

The risk assessment strategy can also be used to make risk-based decisions on an ad-hoc basis.

In addition to the above requirements, the VP of IT shall ensure that the effectiveness of DCCC's key security safeguards, including those to detect actual and attempted attacks on, or intrusions into, information systems, are regularly tested/monitored.

7. Compliance

Failure to comply with this policy may result in sanctions in accordance with the Employee and/or Student Handbook and applicable laws and regulations, which may include termination of employment or enrollment. It is the responsibility of every individual user to report any known violations to the VP of IT or the VP of Finance and Administration. Authorized Users who wish to report suspected violations confidentially, or who are concerned about potential retaliation, may do so through the College's Whistleblower Policy, which includes an anonymous reporting hotline at 855-832-5551 or www.dccchotline.ethicspoint.com (https://secure.ethicspoint.com/domain/media/en/gui/37551/).

Inadvertent misuse of the College's computing systems, for example unintentional overload of systems or excessive disk consumption, will be handled by procedures of the College's Office of Information Technology.

- Violations by students will be reported to the Vice President of Student Affairs for review and resolution according to the procedures of the Student Code of Conduct as stated in the DCCC student handbook.
- Violations by staff will be reported to the Vice President of Finance and Administration, the staff member's supervisor, and to the Vice President of Human Resources for review and resolution in accordance with the College's personnel policies.
- Violations by the public will be reported to the Vice President of Finance and Administration for review and resolution. Penalty for violation may range from prohibition of access to DCCC's systems and facilities to the notification of law enforcement authorities.
- Account privileges and access to specific systems, services, or devices may be suspended, disabled, restricted, or terminated while a reported violation is under review or where a violation has occurred or is suspected, pending investigation and resolution.

Organizational compliance and efficacy of this Policy shall be reviewed periodically, as deemed necessary by the VP of IT. The review, per this Policy, will include the following minimum attributes:

- Updates upon significant changes to the system or organizational requirements or in response to the results of a risk assessment;
- Consistency in implementation;
- Maintenance of implementing procedures; and
- Compliance with applicable laws and regulations.

Exceptions

Exceptions must be approved and documented by the DCCC Office of Information Technology. All exceptions shall be documented and reviewed during the next upcoming Risk Assessment. Please see the Information Security Policy (ISP.9.1) for additional information.

8. References

- ISO 27001:2022 Information security management systems — Requirements
- NIST SP 800-53 r. 5 Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-37 r. 2 Risk Management Framework
- 16 C.F.R. Sections 314.3-314.4 (FTC Safeguards Rule)