9.5 NETWORK AND APPLICATION SECURITY

Original Date of Issue: 5/20/2026

1. Purpose

This Network and Application Security Policy ("Policy") defines the governance requirements for implementing changes to the Delaware County Community College ("DCCC") Information Technology ("IT") systems and environments. Maintaining a secure information environment is a DCCC strategic objective. The Board of Trustees demonstrates its commitment to information and cyber security through the maintenance of this Policy and associated policies and procedures.

2. Scope

This Policy applies to all authorized users of DCCC who are provided access to DCCC information systems and environments. It defines the network security 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

Assets or Information Assets are data or information that belongs to DCCC and the hardware, software, firmware, or physical (i.e., hardcopies) assets that contain or support in protecting or operationalizing that data or information.

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 AVP of IT (defined below).

Responsible

Assistant Vice President of Information Technology ("AVP of IT"): The AVP of IT is responsible for the day-to-day operation of this policy and implementing procedures.

Supportive

IT Team: The IT Team is responsible for managing and monitoring the DCCC network and applications according to this Policy and implementing procedures.

Consulted

Department Heads: Department heads 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. Network Management

DCCC uses zero-trust principles to secure its network. It maintains a perimeter to ensure clear denotation of in-scope and out-of-scope assets. The internal network is segmented with a level of granularity as deemed appropriate by the AVP of IT. Authentication shall occur prior to authorizing a communication.

Perimeter Security

DCCC establishes a perimeter between DCCC-controlled assets and third-party assets. The perimeter shall be protected via implementation of hardware, software, and/or firmware tools (i.e., firewalls, DMZ, web filtering). All devices must be pre-approved prior to connecting to the network and may only connect with approved protocols.

All connections to the information system at the perimeter (including physical and logical connections, remote connections, and wireless access points), shall be reviewed and approved via the Change Management process (see 9.8). All remote access must be through a virtual private network ("VPN") connection, unless otherwise approved by the AVP of IT.

DCCC shall monitor the flow of information at the perimeter (i.e., DMZ/sandboxing, data loss prevention, network traffic monitoring). Sensitive and Confidential Information, including personally identifiable information protected under applicable data protection laws, shall be encrypted prior to leaving the network boundary unless an effective alternative mechanism was approved by the AVP of IT (see 9.11 Encryption and Key Management).

The perimeter is documented in the network diagram per the Asset and Data Management Policy (see 9.9) and changes to the perimeter must adhere to the Change Management process (9.8 Configuration and Change Management).

Network Management

DCCC segments its network to enforce its access policy. Devices not managed by DCCC shall only be able to connect to designated VLANs. Sensitive and Confidential data shall not be stored on these VLANs unless otherwise approved by the AVP of IT (see 9.9 Asset and Data Management).

All devices shall be managed by DCCC prior to connecting to its network outside of the unmanaged Bring Your Own Device (BYOD) network or unless otherwise approved by the AVP of IT.

Network and architecture engineering activities shall utilize secure architecture engineering techniques guided by zero-trust principles. The network should be segmented between operational units. When implementing network segmentation, the IT department shall consider the following minimum factors:

- Making segmentation as granular as feasible and minimizing implicit trust zones.
- Mitigating the effects of natural disasters or security incidents.
- Enabling the ability to implement least privileged access.
- Ensuring minimal disruption during maintenance.
- Separation of production, testing, and development environments.

Network connection sessions shall be reauthenticated periodically. Session inactivity timeouts shall be configured by the AVP of IT based on role, system sensitivity, and operational requirements. The AVP of IT shall document the applicable timeout standards in implementing

procedures. Higher-risk systems and privileged accounts shall be configured with shorter inactivity thresholds than standard user sessions. Endpoints will be monitored for malicious activity and vulnerabilities per the Vulnerability Management Policy (see 9.6 Vulnerability and Patch Management).

All network devices should conform to the secure baseline and changes shall be made pursuant to the Change Management Process (see 9.8 Configuration and Change Management).

WiFi access shall be segmented to support information security and the Principle of Least Privilege. DCCC shall maintain separate wireless network segments for staff, students, and guests. Staff wireless access shall require authentication and provide access to DCCC managed resources consistent with role-based access controls. Student wireless access shall be provisioned to support academic use while restricting access to administrative systems. Guest wireless access shall be isolated from all DCCC internal networks and managed systems, with the exception of DNS, DHCP, NTP and access to publicly available DCCC-hosted web services. The AVP of IT shall determine the appropriate level of segmentation and access controls for each wireless segment based on periodic risk assessment.

6. Application Management

All applications shall be managed and inventoried by the DCCC IT department or an authorized delegate. Configurations should align with the secure configuration standards established by the Configuration and Change Management Policy (see 9.8). Connections between applications should be verified (i.e., requiring validation and monitoring communications).

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 AVP 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.

- 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 AVP of IT. The review, per the Information Security Policy (9.1), 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 (9.1) for additional information.

8. References

- 9.1 Information Security Policy
- 9.6 Vulnerability and Patch Management
- 9.8 Configuration and Change Management
- 9.9 Asset and Data Management
- 9.11 Encryption and Key Management
- 9.12 Third Party and Vendor Management
- 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)