9.4 IDENTITY AND ACCESS MANAGEMENT

Original Date of Issue: 5/20/2026

1. Purpose

This Access and Account Management Policy ("Policy") defines the governance requirements for identity and privileged management, authentication, and local, remote, and physical access 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 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/) for additional definitions

Multifactor Authentication ("MFA") is an infrastructure that requires two or more authentication methods to confirm the identity of authorized users (i.e., push notifications, hardware tokens, biometrics, etc.).

Remote Workers are authorized users who are approved to work remotely, or access DCCC remotely to fulfill their job responsibilities.

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

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

Department Heads: Department Heads are responsible for all ensuring all personnel are appropriately trained on the information within this Policy.

Information Technology ("IT") Department: Implements access provisioning, removal, and reviews in line with relevant procedures.

Human Resources ("HR") Department: Implements personnel screening prior to access provisioning and works with the IT team to modify access levels.

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. Identity and Access Management

DCCC manages identities of Authorized Users through the Users' entitlement lifecycle. The AVP of IT may document implementing procedures for the Policy provisions below. The AVP of IT shall implement technical and physical access controls, as described below, to ensure access to only authorized users and limit access to only the minimum information needed to fulfill their job functions. The AVP of IT shall periodically review the adequacy of these controls.

Governance

DCCC uses the Principle of Least Privilege to provide access. All access must be approved with appropriate business justification.

Account Management

All accounts shall be centrally managed by DCCC IT, except as authorized by the VP of Finance and Administration. Accounts not managed by IT shall be assigned to an owner responsible for ensuring compliance of the asset.

Where deemed appropriate by the AVP of IT Single Sign On ("SSO"), SSO should be configured, and the accounts should be federated into the SSO plane. The creation of any user account, including those on local computers, is prohibited, unless expressly approved by the AVP of IT. Users are required to authenticate as themselves to all DCCC systems. Use of generic accounts or service accounts for physical or console access must be authorized by the AVP of IT.

User-Level Access

Each user shall receive a unique ID to enable audit and accountability measures. Identifiers shall not be reused. User accounts are for the express use of the individual it has been assigned to. In some instances, individuals may be required to authenticate to systems not owned or managed by DCCC. In these instances, it is the responsibility of the individual to maintain the fidelity of that user credential (name and password).

In all cases, access to DCCC systems should only be granted with the least privileges required to perform the individual's duties or to fulfill an educational need (Principle of Least Privilege). Users must not allow anyone else to use their user ID/token and password on the DCCC IT system.

Privileged Access Management

The use of elevated privileged accounts by unauthorized individuals is prohibited. Users authorized for privileged accounts shall only use privileged accounts where necessary and standard user accounts where elevated privileges are not necessary to complete their job duty.

In some instances, DCCC will create and manage central accounts for the purpose of administration (service accounts). Use or access to these accounts are prohibited by unauthorized personnel and creation

of service accounts by non-IT individuals is prohibited. Use of utility programs shall be restricted to those with explicit authorization.

If deemed necessary by the AVP of IT, privileged users shall receive additional training tailored to their role. Roles for critical tasks shall be assigned to observe Separation of Duties. Privileged users must maintain their authentication credentials in an approved password vault. All administrative system access shall take place in an approved virtual environment unless there is a documented exception.

Access by Third Parties

Third parties may sometimes require access to DCCC systems to fulfill a business or educational need (see 9.12 Third Party and Vendor Management). Access shall be provisioned per the Principle of Least Privilege in accordance with that need. Contractual agreements shall include requirements to comply with minimum security measures as deemed required by the DCCC and/or follow DCCC policies and procedures. Third parties should attest to commensurate screening and training in lieu of completing those aspects prior to obtaining access. The AVP of IT has the authority to deny third-party access based on risks posed by lack of training and screening attestation. Access is removed when no longer required or upon termination of the agreement term.

Access Provisioning

The AVP of IT may establish and maintain procedures for access provisioning and shall ensure workflows are created for secure account creation. DCCC uses a ticketing system to manage access provisioning workflows. Prior to receiving access, each user shall receive a level of screening proportionate to their role and acknowledge the Acceptable Use Policy (see 9.2). Department heads shall ensure there is a business or educational justification for the access request recorded on the ticket. Within 45 days of access provisioning, each Authorized User shall complete all required training. Failure to complete the training shall result in access removal at the discretion of the AVP of IT.

Access Level Requirement Changes

The AVP of IT shall establish and maintain procedures to ensure effective and timely access revisions in the event access is no longer needed or access level requirements are reduced.

If an Authorized User's role changes, the User's manager shall notify IT of new access requirements and existing access that is no longer necessary. Access shall be promptly adjusted per the Principle of Least Privilege.

In the event of an Authorized User separation (i.e., graduation, termination of enrollment or employment, etc.), access shall be revoked within 24 hours after separation. For an Authorized User hostile termination, access shall be revoked within one business hour of notification.

Auditing

Access audits and entitlement reviews shall occur periodically within timeframes determined by the VP of Finance and Administration and AVP of IT. The audit scope shall include privileged and non-privileged access. All records shall be maintained per the Data Retention Policy (see 9.9 Asset and Data Management). The AVP of IT may establish procedures for access audits and entitlement reviews.

6. Authentication Management

Multifactor Authentication ("MFA")

Multifactor Authentication ("MFA") is required on all assets to authenticate user identity, unless an alternative equivalent measure is approved in by the AVP of IT. Where possible, DCCC implements passwordless authentication. This is effectuated via different authenticator tokens (i.e., push notification, biometrics, etc.).

Authentication credentials are revoked when the user is no longer authorized to be on the DCCC system. The AVP of IT shall ensure accounts are locked after a defined number of incorrect attempts.

Password Management

Authentication shall be required at defined barriers to prevent lateral movement of bad actors in DCCC systems. Users, devices, and applications must be authenticated at these barriers. DCCC securely stores and encrypts passwords.

DCCC maintains a password standard that establishes a minimum complexity and expiration cadence. Temporary passwords must be changed immediately upon logging on. Authorized users shall not use their DCCC system passwords for personal devices and applications. The AVP of IT may document procedures for securely creating and resetting passwords.

Authorized users must protect their authentication information from unauthorized disclosure. Authorized Users must not share their credentials with others or write passwords down. Passwords may be stored in a DCCC-approved secure password manager. Upon becoming aware, Authorized users must immediately report compromise of their password to the Information Security team.

7. Physical Security

DCCC maintains physical security controls as part of its information security program. In addition, all physical premises shall comply with applicable building codes and regulations.

Access Control

DCCC controls and monitors the physical barriers of its premises that contain sensitive DCCC information. Access shall be granted based on need related to the user's role (role-based access). Access to ingress/egress points should be monitored (i.e., via badge readers, security officers, CCTV, etc.).

Enhanced access controls should be documented and applied to all sensitive IT infrastructure and physical manifestations of Sensitive information (see 9.9 Asset and Data Management). Data centers should have all ingress/egress points locked and access logged.

DCCC maintains a clear desk and clear screen policy. While not working with DCCC information, that information shall be securely stored. Offices or rooms with critical assets should have an enhanced level of security based on a risk assessment (see 9.1 Information Security Policy).

Environmental Security

Physical premises are maintained to ensure the protection of critical assets. Additionally, DCCC considers controls and planning for business continuity in the event that physical premises are affected enough to cause business disruption (see 9.7 Incident Response and Business

Continuity). Key information assets should be fortified against potential damage from environmental factors (i.e., flood, fire, etc.).

Equipment shall be properly maintained to ensure the protection of critical data and safety of personnel. Safety regulations shall be observed at all times and equipment cabling shall be protected and properly maintained. All electronic equipment hosting or supporting critical assets shall implement appropriate surge protection.

Visitor Security

Visitors may not access Restricted Areas without an escort or prior approval. For visitors accessing areas with critical assets without an escort, a background check or attestation of prior screening commensurate to DCCC screening requirements shall be required if deemed necessary by the AVP of IT.

Monitoring

The physical premises shall be monitored for unauthorized activity. The AVP of IT may establish procedures and security controls to monitor and log user activity and to detect unauthorized access, use, or tampering of Sensitive and Confidential information, including personally identifiable information protected under applicable data protection laws. The AVP of Facilities shall periodically review physical access to ensure it is still necessary.

8. Remote Access

DCCC allows remote access and work from home under a set of conditions as defined by this Policy. The AVP of IT may document procedures for the identification, management, and monitoring of remote eligible access and functions.

Remote Access Requirements

Only pre-approved remote connections shall be permitted on DCCC systems. All remote access shall require multifactor authentication ("MFA"). All remote traffic that may contain Sensitive and Confidential information, including personally identifiable information protected under data protection laws, shall be encrypted (i.e., via virtual private network ("VPN")) or another effective alternative control as approved by the AVP of IT.

Only assets that enable DCCC management of data and configurations or assets otherwise approved by the AVP of IT shall be allowed to connect remotely to DCCC systems. Remote connections shall be established via approved protocols. The use of non-approved protocols is prohibited. Remote connections shall be terminated after a period of inactivity in accordance with Configuration and Change Management (see 9.8).

Remote maintenance shall be limited to authorized administrators for authorized business reasons. Maintenance shall be effectuated in a secure manner.

Remote Work and Access

All remote workers, regardless of the nature or frequency of their remote access, must comply with the security requirements governing remote access as documented in the Remote Work Security Standards (see 9.2 Appendix A). Remote workers must ensure that they are working in a secure environment and use secure networks while accessing DCCC systems remotely.

Monitoring and Review

All remote access shall be documented and periodically reviewed in accordance with Centralized Logging and Monitoring (see 9.10).

9. 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.

10. References

- 9.1 Information Security Policy
- 9.2 Acceptable Use Policy
- 9.7 Incident Response and Business Continuity Policy
- 9.8 Configuration and Change Management
- 9.9 Asset and Data Management

- 9.10 Centralized Logging and Monitoring
- 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
- 16 C.F.R. Sections 314.3-314.4 (FTC Safeguards Rule)