700.4 Authentication and Credential Security Policy

Policy Title: Authentication and Credential Security Policy
Policy Number: 700.4
Responsible Office: Information Technology Services (ITS)
Approval Authority: Administrative Council; President's Cabinet (Final Approval)
Applies To: All users of College-managed systems
Alignment: FERPA; GLBA; NIST SP 800-63 Digital Identity Guidelines; recognized cybersecurity authentication frameworks (as updated)
Effective Date: May 2026
Current Version: 1.0.0
Supersedes: None
Next Scheduled Review: January 2027

I. Overview and Purpose

The purpose of this policy is to establish requirements for secure authentication to College-managed systems, networks, and services.

Strong authentication practices protect institutional data, reduce the risk of unauthorized access, and support compliance with regulatory and operational security requirements.

Technical authentication controls, including credential length, authentication factors, lockout protections, and other operational requirements, are defined in the ITS Authentication Standard (700.4.1).

II. Scope

This policy applies to:

- Faculty
- Staff
- Students
- Contractors
- Student workers
- Third-party users granted access to College systems

It applies to all systems and services that authenticate users through College-managed identity systems or that process institutional data.

III. Credential Protection

Users are responsible for protecting authentication credentials issued for access to College systems.

Users shall not:

- Share passwords, passphrases, or authentication credentials with any other individual
- Approve Multi-Factor Authentication (MFA) requests they did not initiate
- Store credentials in unsecured locations
- Attempt to bypass authentication controls or identity protections

Users must immediately report suspected credential compromise in accordance with the Incident Response and Security Incident Management Policy (780.1).

IV. Authentication Requirements

All College-managed systems must implement authentication controls appropriate to the sensitivity of the systems and the institutional data they protect.

Authentication credentials must meet technical requirements as defined in the ITS Authentication Standard (700.4.1).

Multi-Factor Authentication (MFA) shall be required for systems and accounts identified by ITS as presenting elevated security risk, including administrative accounts, remote access systems, and services containing Confidential or Restricted institutional data.

V. Remote and Off-Campus Access

Access to College systems, applications, or institutional data from off-campus or external networks must be secured through College-approved authentication and access controls.

Information Technology Services (ITS) will enforce appropriate access methods (e.g., secure remote access solutions, conditional access, or Zero Trust Network Access (ZTNA)) based on system sensitivity, data classification, and institutional risk.

Systems that store or process Confidential or Restricted institutional data may require enhanced access controls, including Multi-Factor Authentication (MFA), device compliance requirements, network restrictions, or additional identity verification measures.

VI. Credential Security

Authentication credentials must be protected using secure authentication protocols and storage mechanisms consistent with the ITS Authentication Standard (700.4.1).

Systems must not store authentication credentials in plain text and must transmit authentication data only through encrypted communication channels.

VII. Identity Provider and Authentication Services

Authentication for institutional systems shall be managed through College-approved identity services where technically feasible.

ITS is responsible for configuring and maintaining authentication technologies, including identity providers, Single Sign-On (SSO) services, and Multi-Factor Authentication (MFA) systems.

VIII. Compromised Credentials

When authentication credentials are suspected or confirmed to be compromised, Information Technology Services (ITS) may require immediate credential reset, temporary authentication disablement, or other technical containment actions necessary to protect institutional systems.

Emergency containment actions performed by ITS are temporary protective measures and do not constitute disciplinary action.

Administrative access removal actions, including Account Suspension (AS), are governed by the Data Governance and Security Oversight Policy (735.0) and may only be authorized by designated administrative authorities.

Such actions may be taken as part of incident containment under the Incident Response and Security Incident Management Policy (780.1).

IX. Enforcement

Violations of this policy may result in corrective action, access restriction or removal, disciplinary action in accordance with College policy, referral to appropriate administrative offices, or other administrative measures as required by applicable law.

Technical enforcement actions may be implemented in accordance with the Data Governance and Security Oversight Policy (735.0) and the ITS Enforcement and Escalation Standard (735.0.1)

X. Standards Authority

Information Technology Services (ITS) is responsible for maintaining the ITS Authentication Standard (700.4.1) and may update technical authentication controls as necessary to address evolving security risks, technology changes, or regulatory expectations.

Operational standards must remain consistent with Board-approved policies.

XI. Revisions

This policy shall be reviewed annually to ensure continued accuracy, regulatory compliance, and alignment with institutional practices. Revisions shall follow the College's established approval process, and all individuals are responsible for compliance with the current approved version. Version history shall be maintained in accordance with institutional documentation standards

Version	Date	Description	Approved By
1.0.0	Jan 2026	Initial release of updated Authentication and Credential Security Policy. Supersedes the "Password Security Policy" (Aug 2024).	President's Cabinet