



INFORMATION TECHNOLOGY DEPARTMENT

CYBERSECURITY AND INFORMATION SECURITY POLICY

Dodge City Community College

1. Purpose

Dodge City Community College (DC3) relies on information systems, networks, cloud services, electronic communications, and institutional data to support teaching, learning, student services, administration, research, community engagement, and business operations. This policy establishes the College's commitment to protecting the confidentiality, integrity, and availability of those resources through reasonable administrative, technical, and physical safeguards.

The objectives of this policy are to reduce cybersecurity risk, support regulatory and contractual compliance, preserve continuity of operations, protect the privacy of individuals, and promote shared responsibility for information security throughout the College community.

2. Scope

This policy applies to all College information resources, whether individually controlled or shared, stand-alone or networked, and whether owned, leased, operated, hosted, or contracted by DC3. It applies to:

- All employees, faculty, staff, administrators, student employees, students when using College resources, contractors, volunteers, vendors, and other authorized users.
- All College-owned or managed computers, servers, networks, mobile devices, cloud services, applications, storage systems, telecommunications systems, and associated peripherals.
- Authorized personally owned devices used to access College accounts, systems, or data.
- All institutional data, regardless of format, location, or method of storage or transmission.

3. Policy Statement

DC3 shall maintain a risk-based cybersecurity and information security program appropriate to the size, complexity, resources, and operations of the College. Cybersecurity is a shared responsibility. All users shall comply with this policy, related standards and procedures, and applicable legal, regulatory, and contractual obligations.

4. Authority and Administrative Responsibility

4.1 Board of Trustees

The Board of Trustees provides institutional oversight by adopting this policy and receiving appropriate reports regarding significant cybersecurity risks, compliance, and material incidents.



INFORMATION TECHNOLOGY DEPARTMENT

4.2 President

The President retains executive responsibility for ensuring that appropriate cybersecurity governance and resources are maintained.

4.3 Director of Information Technology/CIO

The Director of Information Technology/CIO serves as the College's designated information security leader and is responsible for administering the cybersecurity program, establishing supporting standards and procedures, coordinating security operations and incident response, and reporting significant risks to executive leadership.

4.4 Data Stewards and Department Leaders

VP's or their designees serve as Data Stewards for information within their areas of responsibility. Data Stewards and department leaders shall authorize access based on legitimate business need, support periodic access reviews, and ensure that departmental practices comply with College requirements.

4.5 Users

Users are responsible for protecting credentials and devices, using only authorized systems and data, completing required training, following security instructions, and promptly reporting suspected incidents.

5. Third-Party Cybersecurity Partnership

DC3 uses qualified third-party cybersecurity providers, including Tandem Cyber Operations, to supplement the College's internal capabilities. Under applicable contracts, statements of work, and College procedures, third-party services may support continuous or active security monitoring, threat detection and response, vulnerability identification and remediation, security assessments, incident response, security awareness activities, and compliance support, including support related to the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and multifactor authentication (MFA).

The Director of Information Technology/CIO retains responsibility for College cybersecurity governance and vendor oversight. Use of an external provider does not transfer the responsibilities of Data Stewards, department leaders, users, or other vendors. Access granted to cybersecurity providers shall be limited to authorized purposes, protected by appropriate contractual terms, and reviewed periodically.

6. Risk Assessment and GLBA Safeguards

DC3 shall maintain a written information security program and conduct periodic risk assessments to identify reasonably foreseeable internal and external risks to student information, financial information, and other protected data. Safeguards shall be selected, implemented, assessed, and adjusted based on identified risk, changes in operations or technology, and the results of security monitoring and testing.

GLBA-related activities shall be documented in supporting standards, procedures, risk records, and reports. The College shall designate responsible personnel, oversee appropriate service providers, and periodically evaluate the effectiveness of safeguards.



INFORMATION TECHNOLOGY DEPARTMENT

7. Data Classification and Handling

Institutional data shall be classified and handled according to sensitivity, legal requirements, and potential harm from unauthorized disclosure, alteration, or loss.

Classification	Description	Examples
Restricted	Disclosure or misuse could create serious legal, financial, operational, or individual harm. Access is strictly limited.	Social Security numbers, financial aid information, payment data, credentials, regulated student or employee records.
Confidential	Nonpublic information requiring protection and access based on job responsibilities.	Personnel records, contracts, internal financial information, nonpublic reports.
Internal Use	Routine operational information not approved for general public release.	Internal procedures, working documents, routine operational communications.
Public	Information approved for public release. Integrity and authorized publication remain important.	Published catalogs, public web content, official announcements.

8. Identity and Access Management

- Access shall be granted according to job responsibilities, approved by appropriate authorities, and limited according to the principle of least privilege.
- User accounts shall be unique to the assigned individual. Shared accounts shall be avoided and used only when specifically approved and controlled.
- Access shall be modified or removed promptly following termination, separation, expiration of affiliation, or a change in job responsibilities.
- Privileged and administrative access shall be restricted, separately controlled where practical, logged, and reviewed periodically.
- Third-party access shall have an identified business owner, defined purpose, and established start and end dates whenever practical.

9. Multi-Factor Authentication

MFA shall be required where technically feasible and appropriate to risk, including for remote access, privileged or administrative access, Microsoft 365 and other cloud services, and systems that store or provide access to Restricted or Confidential data. Users shall not approve unexpected authentication prompts, share authentication factors, or attempt to bypass MFA or other security controls.

10. Security Monitoring, Logging, and Endpoint Protection

DC3 shall maintain security monitoring and protective capabilities appropriate to identified risks. Monitoring may be performed by authorized College personnel and approved third-party providers and may include



INFORMATION TECHNOLOGY DEPARTMENT

endpoint detection and response, network and cloud monitoring, security-event collection, alert investigation, vulnerability scanning, threat intelligence, and audit-log review.

Users should have no expectation that activity conducted through College information resources is private, subject to applicable law and College policy. Monitoring shall be conducted for legitimate operational, security, compliance, and legal purposes.

11. Vulnerability, Configuration, and Patch Management

College systems shall be configured and maintained using approved security baselines when practical. Security vulnerabilities shall be identified, prioritized according to risk, and remediated or otherwise addressed within reasonable timeframes. Unsupported or end-of-life systems shall be upgraded, isolated, replaced, or formally accepted as a documented risk.

12. Security Awareness and Training

Employees and other designated users shall complete cybersecurity awareness training upon assignment and periodically thereafter. Training may include phishing, social engineering, credential protection, data handling, mobile-device security, incident reporting, and safe use of artificial intelligence. Additional role-based training may be required for users with privileged access or responsibilities involving regulated data.

13. Incident Reporting and Response

All users shall immediately report suspected or confirmed cybersecurity incidents to the IT Help Desk or Director of Information Technology/CIO. Reportable events include suspicious messages, suspected phishing, malware or ransomware, account compromise, unexpected MFA prompts, unauthorized access, lost or stolen devices, and improper disclosure of institutional data.

DC3 shall maintain incident response procedures addressing preparation, detection, analysis, containment, eradication, recovery, documentation, communications, and post-incident review. The College may engage Tandem Cyber Operations, legal counsel, insurers, law enforcement, regulators, and other specialists as appropriate. Required notifications shall be coordinated with authorized College leadership and counsel.

14. Encryption and Secure Transmission

Restricted and Confidential data shall be protected in transit and at rest using College-approved encryption or equivalent safeguards when technically feasible and appropriate to risk. Sensitive data shall not be transmitted through unapproved personal accounts, consumer file-sharing services, or other unauthorized methods.

15. Backup, Recovery, and Continuity

Critical systems and institutional data shall be backed up according to documented standards. Backups shall be protected from unauthorized access and alteration, retained according to operational and legal requirements, and tested periodically for recoverability. Disaster recovery and business continuity procedures shall identify priorities, dependencies, responsibilities, and recovery objectives for critical services.



INFORMATION TECHNOLOGY DEPARTMENT

16. Mobile Devices, Remote Access, and Personally Owned Devices

Devices accessing College systems shall use reasonable safeguards, including supported software, screen locking, current security updates, and approved malware protection where applicable. Remote access shall use College-approved methods. Lost, stolen, or compromised devices that access College accounts or contain institutional data shall be reported immediately. DC3 may restrict access from devices that do not meet security requirements.

17. ThirdParty and Cloud Service Risk Management

Technology vendors and cloud services that store, process, transmit, or access institutional data shall undergo a security and privacy review appropriate to risk before purchase or implementation whenever practical. Contracts should address data ownership, confidentiality, security controls, incident notification, regulatory obligations, subcontractors, data return or destruction, and termination of access. Technology acquisitions shall be coordinated with Information Technology and the appropriate Data Steward.

18. Compliance

The College shall maintain practices that support compliance with applicable legal, regulatory, contractual, and policy requirements, including, as applicable:

- Family Educational Rights and Privacy Act (FERPA).
- Gramm-Leach-Bliley Act (GLBA) and the Safeguards Rule.
- Payment Card Industry Data Security Standard (PCIDSS).
- Federal Student Aid (FSA) Cybersecurity Compliance Requirements.
- Kansas records, privacy, and breach-notification requirements.
- Health-information requirements when applicable to a College function.
- Applicable contractual, grant, insurance, and Kansas Board of Regents requirements.

Detailed compliance requirements may be maintained in separate standards, procedures, plans, and records that can be updated without amending this board-level policy.

19. Exceptions and Risk Acceptance

Exceptions to this policy must be documented, limited in duration and scope, assessed for risk, and approved by the Director of Information Technology/CIO and the appropriate executive or Data Steward. Compensating safeguards may be required. Exceptions involving material institutional risk shall be escalated to the President or designee.

20. Enforcement

Violations may result in restriction or removal of access, disciplinary action up to and including termination or expulsion, contractual remedies, financial responsibility where permitted, and referral to law enforcement or regulatory authorities when appropriate. Enforcement shall be consistent with applicable College policies, contracts, and law.



INFORMATION TECHNOLOGY DEPARTMENT

21. Related Policies and Supporting Documents

- Series 843, Information Systems Policy.
- Artificial Intelligence Use Policy.
- Social Media Use Policy.
- Incident Response Plan.
- Disaster Recovery and Business Continuity Plans.
- Data Classification and Handling Standard.
- Access Control and Account Management Procedures.
- Vendor Security Review Procedures.

22. Definitions

Cybersecurity Incident: An event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information resource or violates security policy.

Data Steward: The Cabinet member or designee accountable for authorizing access to and appropriate use of data within an assigned area.

Least Privilege: Limiting access to the minimum resources and permissions necessary to perform authorized duties.

Multi -Factor Authentication (MFA): Authentication using two or more different factor types, such as something known, possessed, or inherent to the user.

Restricted Data: Institutional data requiring the highest level of protection because of law, regulation, contract, or significant risk.

Security Monitoring: Authorized collection and analysis of system, network endpoint, application, or cloud activity for security, operational, compliance, or investigative purposes.

23. Review and Revision

This policy shall be reviewed at least every three years and may be reviewed sooner when significant changes occur in law, regulation, technology, threat conditions, College operations, or contracted cybersecurity services. The Director of Information Technology/CIO may issue and revise supporting standards and procedures consistent with this policy.

Policy Owner

Director of Information Technology/CIO

Administrative reference: Tandem Cyber Operations public service information is available at tandemcyber.co. Specific services are governed by DC3 contracts and statements of work.