DOANE

TECHNOLOGY INFORMATION SECURITY PROCEDURES

Purpose

These procedures are established to implement and support Doane University's Information Security Policy by translating its principles into specific, operational practices. Together with the University's Information Security Program (ISP), these procedures define the processes, responsibilities, and technical safeguards required to secure the University's technology environment. These ensure that security controls are consistently implemented, monitored, and improved to protect Institutional Data, safeguard Covered Information under the Gramm-Leach-Bliley Act (GLBA), maintain system reliability, and support compliance with legal, regulatory, and contractual requirements.

Industry Standards and Definitions

Doane University's Information Security Program is designed to support compliance with applicable legal and regulatory requirements, including the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA) where applicable, the Payment Card Industry Data Security Standard (PCI-DSS) where applicable, and relevant state breach notification and privacy laws. The following standards serve as the foundation for all requirements:

- **NIST SP 800-171**: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- **Center for Internet Security (CIS) Controls v8**: A prioritized set of safeguards to mitigate the most prevalent cyber threats
- **ITIL Service Management**: A framework of best practices for incident, change, and service delivery management to ensure consistent and reliable technology operations.
- **ISP Coordinator:** The Information Security Program (ISP) Coordinator is the designated individual responsible for overseeing Doane University's Information Security Program in compliance with the Gramm-Leach-Bliley Act (GLBA) and related regulations.

All security controls, processes, and assessments will be mapped to these standards, ensuring alignment with best practices and regulatory obligations. Doane University contracts a cybersecurity company to support monitoring, testing, and compliance activities.

Scope

These procedures apply to all University-owned, leased, managed, hosted, or contracted information systems, applications, devices, infrastructure, and data environments that store, process, transmit, or provide access to Institutional Data. These procedures apply to faculty, staff, student workers, contractors, temporary workers, third parties, and any other authorized users of University systems or data. These procedures also apply to cloud services, vendor-managed platforms, and outsourced technology services where applicable.

Procedures

Exceptions to these procedures must be documented and approved before implementation whenever feasible. Exception requests must include:

- business justification
- scope and duration of the exception
- risk analysis
- compensating controls
- approval by the appropriate System Owner, Data Owner, Technology Services, and other designated leadership as required

Approved exceptions must include a review date and expiration date and must be re-evaluated at least annually or per Technology Services standard.

Procedures

1. Governance and Risk Management

   Cross-cutting governance aligned to the Information Security Program, GLBA Safeguards Rule, and applicable CIS Controls.

   The University maintains a formal governance and risk management program to ensure that information security risks are identified, evaluated, and managed in accordance with regulatory and operational requirements.

   1.1. Roles and Responsibilities

      1.1.1. The ISP Coordinator oversees the Information Security Program, coordinates assessments, facilitates compliance activities, and reports material risks and control issues to leadership.

      1.1.2. Technology Services implements, operates, monitors, and enforces security controls and supports incident response, vulnerability management, logging, and technical remediation.

      1.1.3. System Owners and Data Owners approve access, participate in risk reviews, support remediation, and ensure systems and data are managed in accordance with these procedures.

      1.1.4. Business Owners are responsible for ensuring that third-party services and business processes align with University security requirements.

      1.1.5. Users must comply with all procedures, complete required training, and report suspected security incidents promptly.

   1.2. Risk Assessment

      1.2.1. Annual risk assessments must be conducted

      1.2.2. Assessments must include systems, data, vendors, and processes

      1.2.3. Risk assessments must evaluate administrative, technical, and physical safeguards, including threats, vulnerabilities, likelihood, and potential impact

      1.2.4. Results must be documented, formally reviewed, and retained

      1.2.5. Risk assessments must be performed at least annually and when significant changes occur, including implementation of new systems, material changes to existing systems, or major third-party service engagements.

1.2.6. Risk assessments must evaluate inherent risk, existing controls, residual risk, and recommended corrective actions.

1.2.7. Results must be used to update remediation plans, control priorities, and leadership reporting.

1.3. Risk Treatment

1.3.1. Risks must be mitigated, transferred, or formally accepted

1.3.2. Risk acceptance must be documented and approved by appropriate leadership

1.3.3. Remediation plans must be tracked to completion

1.3.4. Accepted risks must identify the approving authority, business justification, residual risk, compensating controls, and review date.

1.3.5. Risks that cannot be remediated within required timeframes must be documented through the formal exception or risk acceptance process.

1.4. Control Review

1.4.1. Security controls must be reviewed at least annually

1.4.2. Reviews must also occur following major system changes or security incidents

2. Asset Management

CIS Control 1 – Inventory and Control of Enterprise Assets

The University maintains visibility and control over all enterprise assets to reduce risk and ensure accountability.

2.1. Asset Inventory

2.1.1. The University must maintain an inventory of all enterprise assets

2.1.2. Inventory must include asset owner, location, type, and classification

2.2. Asset Ownership

2.2.1. Each asset must have an assigned owner responsible for its security and lifecycle management

2.3. Unauthorized Assets

2.3.1. Unauthorized devices must be detected and prevented from accessing the network

2.3.2. Detected unauthorized assets must be investigated and remediated

3. Software Asset Management

CIS Control 2 – Inventory and Control of Software Assets

The University manages software assets to reduce vulnerabilities, ensure licensing compliance, and prevent unauthorized applications.

3.1. Approved Software

3.1.1. Only approved software may be installed on University systems

3.1.2. Unsupported or unauthorized software must be removed or formally approved with compensating controls

3.2. Software Inventory

3.2.1. Software inventories must be maintained and reviewed regularly to detect unauthorized or unsupported applications

3.3. Software Installation Controls

3.3.1. End-users may not install software without approval

3.3.2. Software requests must follow formal approval and deployment processes

4. Data Protection and Classification

CIS Control 3 – Data Protection

The University protects Institutional Data based on its sensitivity, regulatory requirements, and business value.

4.1. Data Classification

4.1.1. Data must be classified as Restricted, Confidential, Internal, or Public

4.1.2. Covered Information must be classified as Restricted or Confidential

4.2. Data Handling

4.2.1. Controls must align with the classification level

4.2.2. Data handling must comply with GLBA and other applicable regulations

4.2.3. The University must maintain awareness of where sensitive data is stored, processed, and transmitted

4.3. Encryption

4.3.1. Data must be encrypted at rest and in transit using approved encryption standards

4.4. Data Lifecycle

4.4.1. Data must be retained according to legal, regulatory, and business requirements

4.4.2. Data must be securely disposed of when no longer required

4.4.3. Restricted and Confidential data may only be stored, processed, or transmitted using approved systems and approved security controls.

4.4.4. Sensitive data transmitted electronically must use approved secure transmission methods.

4.4.5. Media containing Restricted or Confidential data must be securely handled, stored, and disposed of using approved methods.

5. Access Control and Identity Management

CIS Controls 5 & 6 – Account Management, Access Control Management

Access to University systems must be controlled to ensure that only authorized users have appropriate access based on business need.

5.1. Account Management

5.1.1. Accounts must be provisioned through documented approval workflows

5.1.2. User accounts must be uniquely assigned to an individual except where a documented business or technical need exists for a shared or service account.

5.1.3. Shared, generic, and service accounts must be approved, documented, limited in use, and reviewed regularly.

5.1.4. Deprovisioning must occur promptly following separation, termination, or role change through documented procedures coordinated with the appropriate business process owners.

5.1.5. Accounts must be automatically disabled after a defined period of inactivity as established by Technology Services standards.

5.2. Authentication

5.2.1. Multi-factor authentication (MFA) is required for administrative accounts, remote access, and systems processing sensitive data

5.2.2. MFA is required for administrative accounts, remote access, email, single sign-on, and systems processing sensitive data, where technically supported.

5.2.3. Authentication mechanisms must follow approved password and identity standards established by the University.

5.2.4. Authorization

5.2.4.1. Role-based access control must be enforced

5.2.4.2. Least privilege must be applied

5.2.5. Access Reviews

5.2.5.1. Access must be reviewed at least quarterly

5.2.5.2. Inappropriate access must be removed and documented

5.2.5.3. Access reviews must be performed by the appropriate System Owner, Data Owner, or delegated business authority, with support from Technology Services.

5.2.5.4. Administrative and privileged access must be reviewed separately and with increased scrutiny.

6. Configuration Management

CIS Control 4 – Secure Configuration of Enterprise Assets and Software

The University maintains secure configurations to reduce vulnerabilities and ensure consistent system security.

6.1. Baseline Configurations

6.1.1. Systems must align with CIS Benchmarks

6.1.2. Secure configuration standards must be established for servers, workstations, network devices, cloud services, and other supported enterprise technologies, based on CIS Benchmarks where feasible.

6.1.3. Deviations from approved baselines must be documented and approved.

6.2. System Hardening

6.2.1. Unnecessary services and features must be disabled

6.2.2. Default accounts must be removed or secured

6.3. Change Management

6.3.1. All changes must follow formal ITIL-aligned change management processes

6.3.2. Changes must be documented, reviewed, approved, and tested

6.3.3. Emergency changes must be documented and reviewed after implementation.

6.3.4. Security-impacting changes must include appropriate testing and validation prior to production deployment whenever feasible.

7. Vulnerability and Patch Management

CIS Control 7 – Continuous Vulnerability Management

The University maintains a proactive vulnerability management program to identify and remediate security weaknesses.

7.1. Vulnerability Scanning

7.1.1. Regular vulnerability scans must be conducted across systems and networks

7.1.2. Scan results must be documented and reviewed

7.1.3. Vulnerability scanning frequency must be based on system risk, exposure, and criticality.

7.1.4. Internet-facing systems and critical systems must be prioritized for more frequent assessment.

7.2. Remediation

7.2.1. Critical vulnerabilities must be remediated within 7–15 days

7.2.2. High vulnerabilities must be remediated within 30 days

7.2.3. Remediation timelines may be accelerated based on risk and active threats

7.2.4. Remediation may include patching, configuration changes, compensating controls, isolation, or documented risk acceptance.

7.2.5. Unsupported systems must have a documented mitigation, replacement, or retirement plan.

7.3. Patch Management

7.3.1. Security patches must be applied based on risk prioritization and system criticality

8. Logging and Monitoring

CIS Control 8 – Audit Log Management

The University maintains logging and monitoring capabilities to detect, investigate, and respond to security events.

8.1. Audit Logging

8.1.1. Systems must log authentication, access, and administrative activity

8.1.2. Logging must include, as applicable, authentication events, authorization events, administrative actions, privileged account activity, system changes, and security events.

8.1.3. Systems generating audit logs must use reliable time synchronization.

8.2. Log Protection and Retention

8.2.1. Logs must be protected from unauthorized access or modification

8.2.2. Logs must be retained in accordance with regulatory and operational requirements

8.3. Monitoring and SIEM

8.3.1. Logs must be monitored through automated tools or regular review

8.3.2. A centralized SIEM must be used to detect anomalous or suspicious activity

8.3.3. Monitoring responsibilities performed by third-party security providers must be governed by defined service expectations, escalation procedures, and University oversight.

8.3.4. Alerts indicating potentially significant security events must be investigated and escalated according to the Incident Response Plan.

9. Network Security

CIS Controls 12 & 13 – Network Infrastructure Management, Network Monitoring and Defense

The University secures its network infrastructure to prevent unauthorized access and detect threats.

9.1. Network Architecture

9.1.1. Network architecture must be documented and reviewed at least annually or per Technology Services standard.

9.1.2. Remote access must use approved secure methods and MFA.

9.1.3. Wireless networks must use approved encryption and security controls appropriate to the risk and intended use.

9.1.4. Administrative access to network infrastructure must be restricted,

secured, and logged.

9.1.5. Firewall and network security rules must be reviewed at least annually or per Technology Services standard.

9.2. Segmentation

9.2.1. Sensitive systems must be segmented from general-use networks

9.3. Network Monitoring

9.3.1. Network traffic must be monitored continuously for suspicious activity

10. Malware and Endpoint Protection

CIS Control 10 – Malware Defenses

The University deploys endpoint and malware protections to prevent, detect, and respond to threats.

10.1. Endpoint Security

10.1.1. Endpoint detection and response (EDR) must be deployed on all supported systems

10.2. Malware Protection

10.2.1. Systems must use centrally managed malware protection tools

10.2.2. Malware definitions and detection mechanisms must be regularly updated

11. Email and Web Security

CIS Control 9 – Email and Web Browser Protections

The University protects users and systems from threats originating from email and web activity.

11.1. Email Security

11.1.1. Email filtering must detect and block phishing, spam, and malicious attachments

11.2. Web Filtering

11.2.1. Access to malicious or unauthorized websites must be restricted

12. Data recovery and Business Continuity

CIS Control 11 – Data Recovery

The University ensures the availability and recoverability of critical systems and data.

12.1. Backups

12.1.1. Backups must be encrypted and access-controlled

12.1.2. Backups must be tested regularly to ensure recoverability

12.1.3. Critical systems must maintain off-site or protected backups

12.1.4. Backup restoration testing must be documented.

12.1.5. Backup frequency and retention must align with system criticality and business requirements.

12.2. Disaster Recovery

12.2.1. Recovery plans must be documented and maintained

12.2.2. Recovery priorities and responsibilities must be defined

12.2.3. Recovery exercises for critical systems must be conducted at least annually or per Technology Services standard and documented.

12.2.4. Recovery priorities, dependencies, roles, and communication expectations must be defined.

13. Vendor Risk Management

CIS Control 15 – Service Provider Management

The University manages third-party risk to protect Institutional Data and ensure compliance.

13.1. Vendor Assessment

13.1.1. Vendors handling sensitive data must be reassessed at least annually

13.1.2. Assessments must evaluate security practices, data handling, and compliance posture

13.1.3. Vendors must be assessed prior to contract execution, renewal, or material scope change when they store, process, transmit, or access Institutional Data or University systems.

13.1.4. Due diligence may include security questionnaires, audit reports, attestations, penetration test summaries, breach history, insurance review, or other evidence appropriate to the level of risk.

13.2. Contract Requirements

13.2.1. Contracts must include data protection, confidentiality, and breach notification requirements

13.2.2. Vendors must comply with University security requirements and applicable regulations

13.3. Vendor Monitoring

13.3.1. Vendor access must be limited, monitored, and reviewed at least annually or per Technology Services standard.

13.3.2. Significant changes or incidents must trigger reassessment

13.3.3. Significant vendor incidents, security control changes, or service model changes must trigger reassessment.

13.3.4. Vendor owners must be identified for high-risk or sensitive vendors.

14. Application Security

CIS Control 16 – Application Software Security

The University integrates security into application development and management processes.

14.1. Secure Development

14.1.1. Secure coding practices must be followed

14.1.2. Development and production environments must be separated

14.1.3. Access to development, test, and production environments must be appropriately segregated.

14.1.4. Secrets, credentials, and keys used in application development and deployment must be protected using approved methods.

14.2. Secure Testing

14.2.1. Applications must be tested for vulnerabilities prior to deployment

14.2.2. Testing may include code review, scanning, and penetration testing

14.2.3. Security findings must be tracked and remediated prior to production deployment based on risk.

14.2.4. Third-party applications and integrations must be evaluated for security risk prior to implementation.

15. Incident Response

CIS Control 17 – Incident Response Management

The University maintains an incident response capability to detect, respond to, and recover from security incidents.

15.1. Incident Response Plan

15.1.1. An Incident Response Plan must be documented and maintained

15.1.2. Roles, responsibilities, and escalation procedures must be defined

15.1.3. The Incident Response Plan must be tested at least annually or per Technology Services standards through tabletop exercises or other appropriate methods.

15.1.4. Significant incidents must undergo post-incident review to identify lessons learned and needed control improvements.

15.2. Incident Reporting

15.2.1. Incidents must be reported internally within 24 hours of discovery

15.2.2. Workforce members must report suspected or confirmed incidents promptly through approved channels.

15.2.3. Technology Services and the ISP Coordinator must evaluate incidents for legal, regulatory, contractual, and operational reporting obligations.

15.3. Response and Recovery

15.3.1. Incidents must follow defined containment, eradication, and recovery procedures

15.3.2. Incident response activities must align with GLBA, FERPA, and applicable

breach notification laws

16. Security Awareness and Training

CIS Control 14 – Security Awareness and Skills Training

The University promotes security awareness to reduce human risk factors.

16.1. Training Requirements

16.1.1. Security awareness training is required upon onboarding and annually thereafter

16.1.2. Role-based training must be provided where appropriate for privileged administrators, developers, managers with approval authority, and personnel handling sensitive data.

16.2. Phishing Simulations

16.2.1. Phishing simulations must be conducted at least annually or per Technology Services standard to reinforce awareness

17. Compliance and Reporting

Cross-cutting (All CIS Controls)

Documentation and evidence supporting compliance with these procedures, including access reviews, risk assessments, vulnerability remediation records, incident records, vendor assessments, exception approvals, and backup testing results, must be retained in accordance with University record retention requirements and applicable legal, regulatory, and contractual obligations.

17.1. Compliance Monitoring

17.1.1. Compliance must be validated through audits, assessments, and monitoring activities

17.2. Reporting

17.2.1. Regular reports must be provided to appropriate leadership regarding material risks, open remediation items, compliance status, training completion, vendor risk issues, and significant incidents. Reporting cadence must be based on risk and regulatory obligations, and at minimum must support annual program oversight.

18. Continuous Improvement

Cross-cutting (All CIS Controls)

18.1. Metrics and KPIs

18.1.1. Security metrics must be defined and tracked to evaluate control effectiveness

18.2. Program Improvement

18.2.1. Findings from assessments, audits, and incidents must be used to

improve controls and procedures

18.2.2. These procedures must be reviewed at least annually and updated following significant regulatory changes, material control changes, or major security incidents.

19. Appendix A - CIS Controls v8 Information Sheet

This appendix provides a high-level overview of the Center for Internet Security (CIS) Controls v8 adopted by Doane University as part of its Information Security Program. These controls represent a prioritized set of safeguards designed to mitigate cybersecurity risks and support compliance with applicable regulatory requirements, including the Gramm-Leach-Bliley Act (GLBA).

Cross References

1. Doane University Information Security Policy
2. Doane University Acceptable Use of Information Systems and Technology Policy
3. Doane University Data Governance Standards
4. Student Privacy Rights (FERPA) Policy

Technology Services may maintain standards, baselines, guidelines, and operational procedures to support implementation of these procedures. Such supporting documents must remain consistent with this document and the University's Information Security Policy.

APPENDIX A - CIS Controls Information Sheet (v8, IG1-IG3)

Purpose

This document provides a high-level summary of the Center for Internet Security (CIS) Controls v8 adopted by Doane University as part of its Information Security Program. These controls represent a prioritized set of safeguards designed to mitigate the most prevalent cybersecurity threats and support compliance with regulatory requirements, including the Gramm-Leach-Bliley Act (GLBA).

This document is intended to supplement the University's Technology Information Security Procedures by providing an overview of each CIS Control and its purpose within the University's cybersecurity framework.

Scope

This information sheet applies to all systems, networks, applications, and data managed or operated by Doane University, including those maintained by third-party service providers.

CIS Control 1 - Inventory and Control of Enterprise Assets

Purpose:
To actively manage all enterprise assets (hardware and network devices) connected to the University environment to ensure that only authorized devices are permitted access.

Summary:
The University maintains a comprehensive inventory of all enterprise assets, including ownership, location, and classification. Unauthorized devices are identified and prevented from accessing the network to reduce exposure to cyber threats.

CIS Control 2 - Inventory and Control of Software Assets

Purpose:
To ensure that only authorized and supported software is installed and executed within the University environment.

Summary:
The University maintains an approved software inventory and uses automated tools to identify unauthorized or unsupported software. Software installation is controlled through formal processes, and unsupported applications must be removed or approved with compensating controls.

CIS Control 3 - Data Protection

Purpose:
To protect sensitive data from unauthorized access, disclosure, or loss.

Summary:
Institutional Data is classified and protected based on sensitivity and regulatory requirements.

Controls include encryption, data lifecycle management, data loss prevention (DLP), and monitoring of access and usage to safeguard Restricted and Confidential data.

CIS Control 4 - Secure Configuration of Enterprise Assets and Software

Purpose:
To establish and maintain secure configurations for systems and applications to reduce vulnerabilities.

Summary:
To establish and maintain secure configurations for systems and applications to reduce vulnerabilities.

CIS Control 5 - Account Management

Purpose:
To manage the lifecycle of user and service accounts to prevent unauthorized access.

Summary:
Accounts are provisioned through approved processes, monitored regularly, and promptly deactivated when no longer needed. Account inventories are maintained, and privileged access is tightly controlled.

CIS Control 6 - Access Control Management

Purpose:
To ensure that access to systems and data is limited to authorized users based on business need.

Summary:
Role-based access control (RBAC) and least privilege principles are enforced. Multi-factor authentication (MFA) is required for sensitive access, and user permissions are reviewed regularly.

CIS Control 7 - Continuous Vulnerability Management

Purpose:
To identify, assess, and remediate vulnerabilities before they can be exploited.

Summary:
The University conducts regular vulnerability scans and prioritizes remediation based on risk. Patch management processes ensure timely updates to systems and applications.

CIS Control 8 - Audit Log Management

Purpose:
To collect, retain, and analyze audit logs for security monitoring and incident response.

Summary:
Systems generate logs for key activities, which are centrally collected and monitored through a SIEM. Logs are protected, retained, and reviewed to detect suspicious behavior.

CIS Control 9 - Email and Web Browser Protections

Purpose:
To reduce the risk of phishing, malware, and web-based attacks.

Summary:
Email filtering, phishing detection, and web content filtering are implemented to prevent malicious content from reaching users and to block access to unsafe websites.

CIS Control 10 - Malware Defenses

Purpose:
To prevent, detect, and respond to malware infections.

Summary:
Endpoint protection and EDR solutions are deployed across systems. Malware detection is continuously updated, and removable media is scanned to prevent infection.

CIS Control 11 - Data Recovery

Purpose:
To ensure timely recovery of data and systems following an incident.

Summary:
The University maintains secure, tested backups of critical systems. Backup processes include encryption, off-site storage, and periodic testing to ensure recoverability.

CIS Control 12 - Network Infrastructure Management

Purpose:
To manage and secure network infrastructure to ensure availability and integrity.

Summary:
Network devices are securely configured, monitored, and maintained. Network architecture is documented, and segmentation is used to protect sensitive systems.

CIS Control 13 - Network Monitoring and Defense

Purpose:
To detect and respond to network-based threats.

Summary:
The University monitors network activity using SIEM, IDS/IPS, and other tools to detect anomalies and respond to potential threats in real time.

CIS Control 14 - Security Awareness and Skills Training

Purpose:
To educate users and reduce human-related security risks.

Summary:
All users complete security awareness training, including phishing education. Training is reinforced through simulations and role-based content.

CIS Control 15 - Service Provider Management

Purpose:
To manage risks associated with third-party vendors.

Summary:
Vendors are assessed before engagement and monitored regularly. Contracts include security and data protection requirements, and vendor access is controlled.

CIS Control 16 - Application Software Security

Purpose:
To ensure that applications are developed and maintained securely.

Summary:
Secure development practices, code reviews, and testing are required for applications. Third-party applications are evaluated for security risks.

CIS Control 17 - Incident Response Management

Purpose:
To effectively detect, respond to, and recover from security incidents.

Summary:
The University maintains an Incident Response Plan, conducts regular testing, and ensures incidents are properly managed, documented, and reviewed.

CIS Control 18 - Penetration Testing

Purpose:
To identify weaknesses through simulated attacks.

Summary:
The University conducts regular penetration testing to evaluate security defenses and validate the effectiveness of implemented controls.