DOANE

TECHNOLOGY INFORMATION SECURITY POLICY

Purpose

This policy establishes the framework for securing Doane University's technology environment by protecting institutional data and information systems, ensuring secure, reliable, and appropriate access, and maintaining compliance with applicable legal, regulatory, and contractual requirements.

The University integrates information security into its operations to support teaching, learning, research, and service while enabling innovation, resilience, and continuity.

Policy

For purposes of this policy, institutional data includes any data created, received, maintained, transmitted, or stored by the University or on its behalf, regardless of format or location.

Doane University maintains a formal Information Security Program (ISP) to identify, assess, and manage risks to institutional data and technology resources. The University applies a risk-based approach to information security that balances innovation, compliance, and operational continuity.

The University implements administrative, technical, and physical safeguards to protect institutional data and systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

All institutional data and technology resources must be governed and protected in accordance with applicable laws, regulations, and University standards, including but not limited to:

- Gramm-Leach-Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA), where applicable
- Payment Card Industry Data Security Standard (PCI-DSS), where applicable
- Applicable state privacy and breach notification laws

The University conducts regular risk assessments and requires that identified risks be mitigated, transferred, or formally accepted by appropriate leadership in accordance with defined procedures.

Technology Services, under the direction of the Chief Information Officer (CIO), is responsible for establishing, implementing, and maintaining the controls, procedures, standards, and governance structures necessary to support and enforce this policy. The CIO designates appropriate roles and responsibilities, including program oversight, system ownership, and data stewardship, to support the Information Security Program.

Supporting procedures, standards, and guidelines are maintained to implement and enforce this policy and must remain consistent with its requirements.

Third-party service providers that access, process, transmit, or store institutional data or University systems must comply with University security requirements and applicable regulatory obligations.

All users are responsible for complying with this policy and associated procedures and must promptly report suspected or confirmed security incidents, unauthorized disclosures, or significant control weaknesses through approved channels.

DOANE

TECHNOLOGY INFORMATION SECURITY POLICY

Applicability

This policy applies to all University technology resources and institutional data, including systems, applications, infrastructure, cloud, hosted, and hybrid environments, devices, platforms, and third-party services that access, store, transmit, or process institutional data.This policy applies to all users, including faculty, staff, students, contractors, third parties, and any other individuals authorized to access University systems or data.

Enforcement

The CIO, or a designated authority, may restrict, suspend, or revoke access to University systems when violations, risks, or threats are identified. Immediate action may be taken to protect institutional resources, with subsequent review and consultation as appropriate.

Enforcement actions will be coordinated with appropriate University offices based on the role of the individual involved and the nature of the violation.

Violations of this policy or associated procedures may result in disciplinary action, loss of access privileges, termination of employment or affiliation, and/or legal consequences, in accordance with University policies and applicable laws.

Exceptions

Exceptions to this policy must be formally documented, include a risk assessment and any compensating controls, an identified review date, and be approved by the CIO or designee. Exceptions must be reviewed periodically to ensure they remain justified, appropriate, and aligned with the University's risk tolerance and compliance obligations.

Cross References

This policy is supported by the following documents and standards:

1. Technology Information Security Procedures
2. Data Classification Procedure
3. Service Provider Management Procedure
4. Data Governance Standards
5. Acceptable Use Policy
6. Information Security Roles and Responsibilities