DOANE

ACCEPTABLE USE OF INFORMATION SYSTEMS AND TECHNOLOGY POLICY

Purpose

This policy establishes the requirements for the responsible, secure, and appropriate use of Doane University's information systems and technology resources. It supports the University's academic, administrative, and operational mission while protecting institutional data, ensuring system integrity, and maintaining compliance with applicable laws, regulations, and University policies.

Policy

For purposes of this policy, technology resources include University systems, networks, accounts, devices, applications, cloud services, communication tools, and Institutional Data. All users of Doane University technology resources—including systems, networks, accounts, devices, applications, and data—must use them in a responsible, ethical, and secure manner consistent with the University's mission. Use of these resources is a privilege, not a right, and requires compliance with this policy and all supporting standards and procedures. Users must use technology only for authorized academic, administrative, research, or incidental personal purposes that do not interfere with University operations, violate law or policy, create **unreasonable risk, or consume excessive resources**; protect University data in accordance with applicable laws and standards; maintain the security of accounts and credentials, including password and multi-factor authentication requirements; use only approved systems and services for University business; comply with applicable laws and regulations, including FERPA, HIPAA, GLBA, FACTA, ADA, and copyright law; and adhere to all University policies and data governance requirements. Users are responsible for activity conducted through their assigned accounts and must take reasonable steps to secure University-managed devices and University data under their control. Prohibited activities include unauthorized access to systems or data; credential sharing; circumvention of security controls; illegal, disruptive, or harmful use; introduction of malware or actions that degrade system performance; unauthorized commercial use; violation of software licenses or intellectual property rights; and misuse of artificial intelligence (AI) tools, including unauthorized disclosure of University data. University technology resources are institutional assets, and the University reserves the right to monitor, access, and review systems and data for security, compliance, legal, and operational purposes in accordance with applicable laws and University policies.

Enforcement and Consequences

The Chief Information Officer (CIO), or designee, may suspend, restrict, or revoke access to technology resources in response to suspected policy violations, security risks, or threats to University systems or data. Immediate action may be taken when necessary to protect institutional operations. Violations may result in disciplinary and/or legal consequences, including:

- **Employees:** Disciplinary action up to termination and/or legal action
- **Students:** Sanctions under the Student Conduct Code, up to dismissal and/or legal action
- **Contractors/Vendors:** Contract termination and/or legal action
- **Guests/Visitors:** Removal from campus and/or referral to law enforcement

Alleged violations will be reviewed in coordination with appropriate University offices. Access may be temporarily restricted during investigations and does not, by itself, indicate a finding of misconduct.

DOANE

ACCEPTABLE USE OF INFORMATION SYSTEMS AND TECHNOLOGY POLICY

Applicability

This policy applies to all faculty, staff, students, contractors, vendors, affiliates, and guests who access or use Doane University information systems or technology resources, to the extent relevant to the access or services provided, whether on campus or remotely. It includes all University-owned, managed, or connected systems, devices, networks, applications, and data.

Exceptions

Exceptions must be formally approved by the Chief Information Officer (CIO) and documented. Approved exceptions are subject to periodic review.

Cross References

This policy serves as the umbrella for supporting documents, including but not limited to:

1. Acceptable Use Procedures
2. Information Security Procedures
3. Doane University Confidentiality and Privacy Standard
4. Doane University Data Governance Standards