DOANE

ACCEPTABLE USE OF INFORMATION SYSTEMS AND TECHNOLOGY PROCEDURES

Purpose

These procedures establish requirements and guidelines for the responsible, secure, and appropriate use of Doane University's information systems, technology resources, and network services. They support the Acceptable Use of Information Systems and Technology Policy by defining user responsibilities, required security practices, and standards of acceptable behavior.

Doane University expects all users of its computing and communication systems to act in a manner that is responsible, ethical, and respectful of the privacy, property, and rights of others. These expectations apply not only within the University community but also to external systems and networks accessible through Doane's technology resources, including the Internet.

Applicability

These procedures apply to all faculty, staff, students, contractors, consultants, affiliates, guests, and other individuals granted access to Doane University information systems or technology resources, including users with limited or restricted access privileges (e.g., alumni or affiliate accounts).

They apply to all University-owned, leased, managed, or contracted computing and communication systems, including hardware, software, cloud services, applications, network infrastructure, telecommunications systems, and any devices or services that connect to or utilize Doane's network or technology environment, whether accessed on campus or remotely.

All users are responsible for complying with applicable federal, state, and local laws; regulatory requirements; contractual obligations; and all other University policies governing the use of information systems and technology resources.

Definitions

- **Information Systems**: Includes Doane-sponsored platforms such as email, messaging services, phone systems, internet and intranet access, academic and administrative portals (e.g., Self-Service, Canvas), and cloud-hosted services.
- **Doane Data**: Refers to information created, accessed, stored, or transmitted on university systems. This includes email, files, databases, student records, HR data, research data, and institutional documents.
- **Technology**: Refers to Doane-owned, leased, or managed information technology infrastructure and systems, including computing hardware, network infrastructure (wired, wireless, and remote access), software applications, cloud services, and related Technology Services services.
- **Artificial Intelligence (AI)**: Technology that allows computers or software to do tasks that usually require human thinking. This includes things like processing language, recognizing patterns, making predictions, or automating decisions.

Procedures

1. Ownership and Monitoring

   Nothing in this procedure alters the ownership of intellectual property as defined in the

Faculty Handbook Intellectual Property Policy.

1.1. All Doane University-provided technology infrastructure, systems, and accounts are the property of Doane University. Data stored within or transmitted through University systems is subject to institutional oversight and control for purposes of security, compliance, and operational continuity. This provision does not alter ownership of intellectual property, academic materials, or scholarly works, which are governed by applicable University intellectual property policies and faculty agreements.

1.2. Doane University reserves the right to determine whether a user is authorized to establish, access, or maintain a particular University information system, technology resource, or institutional data, consistent with role, affiliation, and institutional need.

1.3. Doane University and Technology Services reserve the right to monitor or restrict use of institutional systems to ensure compliance with University policies, security requirements, and applicable laws.

1.4. While Doane University respects the privacy of its community members and complies with applicable privacy laws (including FERPA and HIPAA where applicable), users should understand that University information systems are institutional resources subject to authorized monitoring, access, and disclosure for legitimate educational, administrative, security, and legal purposes. Accordingly, users should not expect personal privacy from institutional oversight when using University systems.

1.5. Activity conducted through University accounts, applications, or networks may generate system logs and audit records, regardless of whether access occurs on a University-owned or personally owned device.

2. User Responsibilities

Access to Doane University information systems and technology resources is a privilege, not a right, and is contingent upon compliance with University policies and procedures.

2.1. Users must comply with all applicable federal, state, and local laws (including, but not limited to, FERPA, HIPAA, GLBA, FACTA, and copyright law), as well as all University policies, procedures, and departmental guidelines governing the use of information systems and technology resources. Where access or resources are provided by a specific department, program, research center, or affiliated unit, users must also comply with any applicable unit-specific policies, data use agreements, and system-specific rules in addition to University and Technology Services requirements.

2.2. Exceptions to these procedures must be documented, risk-reviewed, and approved by the CIO in coordination with Technology Services and other responsible offices as applicable.

2.3. Users must use University-issued accounts when conducting official University business or when representing Doane University in an institutional capacity. This requirement applies to activities performed as part of an individual’s employment, enrollment, or authorized institutional role. It does not extend to personal activities or independent professional service conducted outside the scope of

University responsibilities. Access to information systems is granted based on role and affiliation and may be restricted, suspended, or revoked for policy violations, security risks, or operational necessity.

2.4. Users must maintain the security and confidentiality of their login credentials.

2.4.1. Passwords and other authentication credentials must comply with University authentication standards established and maintained by Technology Services, including password, multi-factor authentication, and related identity security requirements where implemented.

2.4.2. Passwords must not be shared, reused across unauthorized systems, or stored in an insecure manner.

2.4.3. If a user suspects unauthorized access to their account, they must immediately change their password and report the incident to Technology Services.

2.4.4. Multi-Factor Authentication (MFA) is required for access to University systems where implemented. Users must not attempt to bypass or disable MFA controls.

2.5. Users must lock or log out of systems when unattended and take reasonable precautions to prevent unauthorized access to devices and systems under their control.

2.6. Users must promptly report suspected security incidents, policy violations, lost or stolen devices, phishing attempts, system vulnerabilities, or suspected compromises to Technology Services through the Service Center. Reporting procedures are published and maintained by Technology Services. Failure to report known or suspected security risks may result in disciplinary action.

2.7. University computing and network resources are shared institutional assets. Users must not engage in excessive or unreasonable use of system resources (including CPU, storage, memory, or network bandwidth) that degrades performance or restricts access for others. If a user requires substantial computing or storage resources for legitimate academic, service or administrative purposes, they must coordinate with Technology Services in advance.

2.8. Limited personal use of University technology resources is permitted provided that such use:

2.8.1. Does not interfere with academic, service, research, or administrative activities;

2.8.2. Does not consume excessive system or network resources;

2.8.3. Does not violate licensing agreements;

2.8.4. Does not involve operating a personal business or commercial enterprise using University technology resources, except as expressly authorized in writing through appropriate University administrative channels and the CIO or designee;

2.8.5. Does not imply University endorsement of personal activities.

2.8.6. The University reserves the right to restrict or revoke personal use privileges if such use becomes excessive or inconsistent with institutional

priorities.

2.9. Personally owned devices that connect to the University network must comply with applicable security requirements, including current operating system updates, antivirus protections (if applicable), and secure configurations. Devices not connected to the University network are not governed by this procedure; however, users are encouraged to follow responsible computing practices.

2.10. Users are responsible for safeguarding University data under their control and understanding that:

2.10.1. The University cannot guarantee protection against data loss;

2.10.2. Deleted data may remain recoverable through backups or forensic processes;

2.10.3. University systems and data may be subject to legal hold, subpoena, audit, or investigation.

2.10.4. Users should not assume that deleted data is permanently destroyed.

3. Appropriate and Prohibited Uses

University information systems and technology resources are provided to support Doane University's educational, research, service, and administrative missions.

3.1. Appropriate Use

3.1.1. Use of University systems for academic, research, educational, and administrative activities consistent with institutional purposes.

3.1.2. Limited personal use, provided that such use:

3.1.2.1. Does not interfere with University operations;

3.1.2.2. Does not consume excessive system or network resources;

3.1.2.3. Does not violate law, policy, or licensing agreements;

3.1.2.4. Does not imply University endorsement of personal activities.

3.1.2.5. Nothing in this procedure is intended to restrict academic freedom or the lawful expression of ideas.

3.2. Prohibited Uses

The following activities are prohibited. This list is illustrative and not exhaustive. Use of artificial intelligence (AI) systems in violation of the University's Artificial Intelligence Policy, academic integrity standards, or other applicable University policies is prohibited. Users must comply with all institutional requirements governing the authorized and appropriate use of AI technologies. Users must not input, upload, transmit, or otherwise expose confidential, regulated, or otherwise restricted University data to AI tools unless the tool has been approved by the University for that data type and use case.

3.2.1. Unauthorized Recording, AI Notetaking, and Wearable Technologies

3.2.1.1. The use of artificial intelligence (AI)-enabled recording tools, automated notetaking systems, smart glasses, wearable devices, or any technology capable of capturing, recording, transcribing, or

transmitting audio, video, or visual data is strictly prohibited under the following circumstances:

3.2.1.2. Without the explicit knowledge and consent of all participants;

3.2.1.3. In classrooms, meetings, advising sessions, healthcare settings, or other environments where privacy or confidentiality is expected;

3.2.1.4. When such use conflicts with FERPA, HIPAA, or other applicable privacy laws or University policies;

3.2.1.5. When used to capture or reconstruct instructional content, assessments, or academic activities without authorization;

3.2.1.6. When used to monitor, surveil, or record individuals in a manner inconsistent with University expectations of privacy and respect.

3.2.1.7. The use of AI notetaking tools, transcription services, or similar technologies for academic or administrative purposes must be explicitly authorized by the instructor, meeting organizer, or responsible University official, and must comply with all applicable University policies, data governance standards, and legal requirements.

3.2.1.8. Doane University strictly prohibits the use of wearable or ambient recording technologies—including but not limited to smart glasses, hidden recording devices, or passive AI capture tools—for covert or unauthorized recording in any University-related context.

3.2.2. Communications that would be improper or illegal in any other medium are equally prohibited when conducted through University systems, including but not limited to:

3.2.2.1. Harassing, threatening, obscene, defamatory, or discriminatory communications, as defined by applicable University policies and governing law;

3.2.2.2. Libelous statements;

3.2.2.3. Forgery or falsification of electronic communications;

3.2.2.4. Impersonation or misrepresentation of identity;

3.2.2.5. Repeated unwanted communications intended to intimidate or disrupt. This prohibition on impersonation or misrepresentation of identity does not restrict legitimate anonymization, de-identification, pseudonymous activity, or privacy-protective practices conducted for research, academic, or other lawful purposes in accordance with applicable law and University policy.

3.2.3. Unauthorized Access and Security Violations

3.2.3.1. Accessing or attempting to access systems, accounts, files, or data without authorization;

3.2.3.2. Using another individual’s account or credentials without permission;

3.2.3.3. Sharing account credentials in violation of policy;

3.2.3.4. Attempting to guess, capture, or crack passwords;

3.2.3.5. Circumventing or attempting to bypass security controls;

3.2.3.6. Conducting unauthorized scanning, probing, or testing of systems;

3.2.3.7. Installing, operating, or facilitating unauthorized proxy services, servers, routers, or access points;

3.2.3.8. Obtaining elevated privileges without authorization.

3.2.3.9. Authorized system administrators may perform security testing within the scope of their assigned responsibilities.

3.2.4. Malicious or Disruptive Activities

3.2.4.1. Introducing malware, viruses, worms, Trojan horses, or other malicious code;

3.2.4.2. Denying service to other users (e.g., flooding, mail bombing, or other resource exhaustion attacks);

3.2.4.3. Excessive or unreasonable consumption of University system or network resources in a manner that materially degrades performance or availability for other users, or that circumvents established resource allocation controls. Legitimate academic, research, or administrative activities requiring substantial computing, storage, or network resources must be coordinated with Technology Services to ensure appropriate provisioning and system stability.

3.2.4.4. Tampering with, damaging, disabling, or destroying University systems, data, or equipment;

3.2.4.5. Theft or unauthorized removal of University technology equipment.

3.2.5. Misuse of Resources for Commercial or Personal Gain

3.2.5.1. Operating a personal business or commercial enterprise without authorization;

3.2.5.2. Sending unsolicited bulk communications (spam or chain letters);

3.2.5.3. Reselling or redistributing University network services;

3.2.5.4. Hosting commercial advertising or services on University systems without prior approval;

3.2.5.5. Using academic software licenses for commercial purposes in violation of licensing terms.

3.2.6. Copyright and Intellectual Property Violations

3.2.6.1. Unauthorized copying, sharing, downloading, distribution, or use of copyrighted materials, including software, music, films, and digital content;

3.2.6.2. Distribution of software or other licensed materials in violation of license agreements.

3.2.6.3. Violating or failing to respect the intellectual property rights of others.

3.2.6.4. This procedure is not intended to limit lawful “fair use” as permitted under the Copyright Act. Users with questions regarding copyright or intellectual property matters should consult the Office of General Counsel or appropriate University officials.

4. Software and Hardware

4.1. Software management

4.1.1. All software, applications, and cloud-based services used for University business must be approved, procured, and licensed through Technology Services or in accordance with University procurement and data governance procedures.

4.1.2. The installation or use of unapproved, unlicensed, or unauthorized software—including software-as-a-service (SaaS), cloud applications, browser extensions, or locally installed applications—for University business is prohibited.

4.1.3. Software must be used in compliance with applicable license agreements, contractual restrictions, and usage limitations.

4.1.4. Technology Services may restrict, remove, or disable software that presents security, licensing, operational, or compliance risks.

4.1.5. Users must not alter, disable, or circumvent University-installed security controls, endpoint management agents, encryption tools, patching mechanisms, or monitoring software.

4.2. Hardware Responsibilities

4.2.1. University-owned hardware remains the property of Doane University and is subject to asset tracking, inventory management, and security configuration standards.

4.2.2. Users are responsible for the physical security and reasonable care of University-issued equipment.

4.2.3. Lost, stolen, or damaged hardware must be reported immediately in accordance with Section 2.6 (Incident Reporting).

4.2.4. Personally owned devices used to access University systems or data must comply with applicable security standards as outlined in the Network and Device Access section.

4.3. Cloud and External Services

4.3.1. University data must not be stored, processed, or transmitted using unapproved external cloud services, file-sharing platforms, or collaboration tools.

4.3.2. The use of external services for University business must be reviewed for data security, privacy, and contractual compliance requirements prior to use.

4.3.3. Users are responsible for ensuring that University data is not exposed through unauthorized integrations, third-party applications, or automated

data-sharing tools.

4.4. Computer Labs

4.4.1. Lab computers and equipment are institutional resources intended to support academic use.

4.4.2. Users must save files only to approved network storage, not local hard drives.

4.4.3. Food, drink, and tobacco products are prohibited in designated lab areas.

4.4.4. Unauthorized removal of equipment, manuals, or supplies is prohibited.

4.4.5. Technology Services reserves the right to reimage, reset, restrict, or modify lab systems as necessary to maintain security, licensing compliance, and operational integrity.

5. Network and Device Access

Access to Doane University's network and technology infrastructure is restricted to authorized users and approved devices that meet institutional security standards.

5.1. Authorized Network Access

5.1.1. When connecting to Doane University's network infrastructure, users must use only University-approved networks (e.g., DU, Eduroam, BYOD, or other designated secure networks).

5.1.1.1. This provision does not prohibit the use of personal cellular data or external internet connections; however, devices connecting to University systems must comply with applicable security requirements.

5.1.2. Access to the University network requires authentication using University-issued credentials and, where implemented, Multi-Factor Authentication (MFA).

5.1.3. Users must not attempt to bypass network authentication mechanisms or other access control safeguards.

5.1.4. When accessing Doane University systems or data from off-campus locations, users must utilize approved secure access methods (such as University-managed VPN or secure authentication services) where required and must ensure that University-issued devices remain compliant with institutional security standards.

5.2. Device Security Requirements

5.2.1. Personally owned devices must meet University security requirements before connecting to the network. Such requirements may include current operating system updates, security patches, antivirus or endpoint protection software (where applicable), and secure configuration settings.

5.2.2. The University reserves the right to restrict or block network access for devices that do not meet security standards or that pose a risk to the network environment.

5.2.3. Users must not conceal, alter, spoof, or disguise device identifiers, including IP addresses or MAC addresses.

5.3. Unauthorized Network Equipment

5.3.1. The installation or operation of unauthorized networking equipment—including personal routers, wireless access points, hubs, switches, proxy servers, or similar devices—is prohibited without prior approval from Technology Services.

5.3.2. Unauthorized equipment may be removed or disabled to protect network integrity and security.

5.4. Remote Access

5.4.1. Remote access to University systems must occur through approved secure access methods, such as University-managed VPN or other authorized secure gateways.

5.4.2. Remote connections must comply with the same authentication and security requirements applicable to on-campus access.

5.4.3. Devices used for remote access must meet University security standards.

5.5. Account and Session Protection

5.5.1. Users are responsible for safeguarding their accounts and ensuring that authenticated sessions are not left unattended or accessible to unauthorized individuals.

5.5.2. The University may implement technical controls including session timeouts, device registration, network access controls, logging, and monitoring to protect institutional systems and data.

5.6. Hardware Lifecycle Management

5.6.1. Doane University maintains a standard hardware refresh cycle of approximately five (5) years for University-issued computing devices, including laptops and lab computers, subject to budgetary and operational considerations.

6. Laptop and Equipment Checkout

Eligibility for equipment checkout is determined by Technology Services in accordance with institutional policies, operational requirements, and resource availability. Checkout privileges may be limited or denied based on role, funding source, availability, prior misuse, or other institutional considerations.

6.1. Institutional Ownership

6.1.1. All equipment remains the property of Doane University.

6.1.2. Equipment must be used in accordance with University policies and procedures.

6.2. Borrower Responsibility

6.2.1. Borrowers are responsible for the care, security, and timely return of equipment in the condition in which it was issued, normal wear and tear

excepted.

6.2.2. Borrowers must not alter, disable, or remove University-installed security controls, monitoring tools, or management software.

6.2.3. Lost, stolen, or damaged equipment must be reported immediately to Technology Services and, when appropriate, Campus Security or local law enforcement.

6.3. Data Protection

6.3.1. Borrowers are responsible for safeguarding any University data stored on issued equipment and must comply with applicable data protection requirements.

6.3.2. Upon return, equipment may be inspected, reimaged, or wiped in accordance with University security standards.

6.4. Financial Responsibility and Privilege

6.4.1. Loss, damage beyond normal wear and tear, or late return may result in financial charges, holds on accounts, disciplinary action, and/or loss of future checkout privileges.

6.4.2. The University reserves the right to deny checkout privileges for prior misuse or policy violations.

7. Account and Access Controls

Access to University information systems is granted based on institutional role, job responsibilities, and legitimate academic or business need. Access is a privilege and may be modified or revoked at the University's discretion.

7.1. Account Provisioning

7.1.1. User accounts are provisioned based on verified affiliation with the University (e.g., employee, student, contractor, affiliate).

7.1.2. Access permissions are assigned according to role-based access principles and the principle of least privilege. Users are granted only the level of access necessary to perform their assigned duties.

7.1.3. Departments are responsible for ensuring that access requests are appropriate, authorized, and aligned with job responsibilities.

7.2. Account Security and Use

7.2.1. Passwords and authentication credentials must remain confidential in accordance with Section 2.3 of this procedure.

7.2.2. Account sharing is prohibited unless explicitly authorized for documented business purposes and approved by Technology Services.

7.2.3. Users are responsible for all activity conducted under their assigned accounts.

7.3. Account Changes and Deprovisioning

7.3.1. Access privileges must be promptly modified or revoked upon a change in role, transfer, separation from employment, termination of contract, or end

of enrollment.

7.3.2. Supervisors and department heads are responsible for notifying Technology Services in a timely manner of employment or role changes requiring modification or termination of access.

7.3.3. Supervisors are responsible for coordinating the transfer of institutional data and the return of University-issued equipment when access is terminated. Where applicable and consistent with University intellectual property policies, individuals may request access to retrieve personal or scholarly materials prior to account deactivation or through an approved post-separation process.

7.3.4. The University reserves the right to immediately disable accounts when necessary to protect institutional systems, data, or operations.

7.4. Restrictions of Privileges During Investigation

7.4.1. During the investigation of alleged inappropriate, unauthorized, or unlawful activity, the University may temporarily suspend or restrict a user's network, system, or account access if continued access presents a risk to University systems, data, or operations.

7.4.2. Temporary suspension or restriction of access is a protective measure intended to preserve system integrity and prevent further potential misuse. It does not, by itself, constitute disciplinary action or a presumption of wrongdoing.

7.4.3. Access restrictions may remain in effect until the investigation is completed and a determination is made.

7.4.4. Unsubstantiated or insufficient reports of misuse will not result in suspension of access unless preliminary review identifies credible evidence of policy violation or security risk.

8. Privacy and Data Handling

Doane University is committed to protecting the privacy, confidentiality, and integrity of institutional data while maintaining the authority necessary to ensure security, legal compliance, and operational continuity.

8.1. Institutional Access and Monitoring

8.1.1. The University may access, review, monitor, or disclose digital content stored on or transmitted through University systems when necessary to:

8.1.1.1. Maintain system security and integrity;

8.1.1.2. Investigate suspected policy violations or unlawful activity;

8.1.1.3. Respond to emergencies;

8.1.1.4. Comply with legal obligations, subpoenas, court orders, or regulatory requirements;

8.1.1.5. Ensure continuity of operations.

8.2. Respect for Privacy of Others

8.2.1. Users must presume that files, directories, communications, and data belonging to other users are private unless clearly designated as public.

8.2.2. If a user inadvertently encounters information that appears private or confidential, the user must cease access and notify the data owner and/or Technology Services as appropriate.

8.2.3. Users who intentionally grant access to their files or services are responsible for ensuring appropriate protections are maintained for any information not intended for public access.

8.3. Protection of Confidential and Personal Information

8.3.1. Users who access or maintain confidential information—including student records, employee records, financial data, protected health information, or other sensitive data—must comply with all applicable privacy laws, regulations, contractual obligations, and University policies.

8.3.2. Sensitive data must be stored securely, encrypted when appropriate, and transmitted only using approved secure methods.

8.3.3. Access to confidential information must be limited to individuals with a legitimate educational or business need, consistent with the principle of least privilege.

8.4. Access to Faculty, Staff, and Student Data

8.4.1. Electronic data associated with faculty, staff, or student accounts will not be accessed without consent except:

8.4.1.1. In response to a valid subpoena, court order, or legal requirement;

8.4.1.2. During a declared emergency affecting health, safety, or system integrity;

8.4.1.3. As part of a formally authorized University investigation;

8.4.1.4. When necessary to preserve institutional operations (e.g., employee separation or incapacity).

8.4.1.5. When necessary to retrieve or preserve University business records required for operations (e.g., employee separation, extended leave, supervisor-approved business continuity needs), as authorized through appropriate University channels.

8.4.2. Determinations regarding emergency access or investigative access shall be made by authorized officials designated through established University processes by the Chief Information Officer, Legal Counsel, Human Resources, Student Affairs, Academic Affairs, or other appropriate University leadership, as applicable to the circumstances.

8.4.3. When legally permissible and operationally appropriate, affected individuals will be notified of such access.

8.4.4. Information obtained through emergency or investigative access will be used only for legitimate institutional purposes and handled in accordance with applicable laws and policies.

8.5. Data Loss, Retention, and Persistence

8.5.1. While the University implements safeguards to protect data, it cannot guarantee protection against data loss.

8.5.2. Users should be aware that deleted files may remain recoverable through system backups, archival processes, or forensic methods.

8.5.3. University data may be subject to legal hold, subpoena, audit, or investigation, and users must not attempt to delete, conceal, or alter data subject to such requirements.

8.6. Removable Media and External Storage

8.6.1. Removable media and external storage devices containing University data must be protected consistent with applicable data classification and security standards.

8.6.2. The University may assist authorized law enforcement or regulatory authorities in accessing data when legally required.

9. Copyright Compliance

Doane University expects all users of its information systems and technology resources to comply with applicable United States copyright laws, the Digital Millennium Copyright Act (DMCA), and all licensing agreements governing the use of copyrighted materials. The University supports compliance through centralized procurement and licensing controls, training and awareness initiatives, and established DMCA response procedures. The use of artificial intelligence (AI) tools must comply with applicable copyright law and the University's Artificial Intelligence Policy. Users remain responsible for ensuring that materials they upload, reproduce, or distribute through AI systems are used in accordance with applicable law and license terms.

9.1. Compliance with Copyright Law

9.1.1. Users may use, reproduce, display, distribute, or perform copyrighted materials only when such use is permitted by law (including fair use), license agreement, or express permission of the copyright holder.

9.1.2. Unauthorized copying, sharing, downloading, distribution, or public performance of copyrighted materials—including software, music, films, images, textbooks, and digital content—is prohibited.

9.2. Software and License Agreements

9.2.1. Software installed on University-owned or personally owned devices connected to the University network must comply with applicable license agreements.

9.2.2. Users must not install, copy, distribute, or use software in violation of license terms.

9.2.3. Academic or institutional software licenses may not be used for unauthorized commercial purposes unless expressly permitted.

9.3. DMCA and Infringement Notices

9.3.1. The University will respond to properly submitted copyright infringement

notices in accordance with the DMCA and institutional procedures.

9.3.2. The University may remove or disable access to allegedly infringing material and may restrict network access pending investigation.

9.4. Enforcement

9.4.1. Violations of copyright law or licensing agreements may result in disciplinary action under University policies and may expose the individual to civil liability or criminal penalties.

10. Identity Theft Prevention

Doane University maintains a Red Flag Identity Theft Prevention Program in accordance with the Fair and Accurate Credit Transactions Act (FACTA) and applicable federal regulations.

10.1. Red Flag Program Compliance

10.1.1. The University identifies, detects, and responds to patterns, practices, or specific activities (“Red Flags”) that indicate possible identity theft involving covered accounts.

10.1.2. Users who handle covered accounts or personal information must comply with the University’s Red Flag Program requirements and applicable procedures.

10.1.3. Required training must be completed by employees whose responsibilities include access to covered accounts or personal information.

10.2. Protection of Personal Information

10.2.1. Users who access, collect, process, store, transmit, or dispose of personal information as part of their University responsibilities must do so only for authorized institutional purposes and in accordance with applicable law, University policy, and data governance requirements.

10.2.2. Personal information must be limited to the minimum necessary for the business purpose, shared only with authorized individuals, and protected using approved administrative, technical, and physical safeguards.

10.2.3. Personal information must be transmitted, stored, and disposed of using approved secure methods and must not be disclosed, downloaded, or transferred to unauthorized systems, services, or individuals.

10.3. Account and Authentication Safeguards

10.3.1. Protection of login credentials, passwords, and multi-factor authentication devices is critical to preventing identity theft and unauthorized account access.

10.3.2. Users must comply with all account security requirements outlined in Section 2.4 of this procedure.

10.4. Institutional Protective Measures

10.4.1. The University reserves the right to restrict or discontinue communication

with external systems, websites, or services known to harbor phishing operations, spammers, malicious actors, or other security threats.

10.4.2. The University may temporarily or permanently disable systems, services, or network connectivity that present a significant risk to the security or reliability of institutional systems.

10.4.3. Such actions are taken to protect institutional systems, data, and community members and are not intended to restrict lawful expression or punish individuals absent policy violations.

11. Enforcement

Violations of this procedure may result in suspension or termination of access to University information systems, disciplinary action, and/or referral to law enforcement.

11.1. Applicability of University Discipline

11.1.1. Inappropriate or unauthorized use of University technology resources is subject to the general policies and disciplinary procedures applicable to students, faculty, and staff.

11.1.2. Certain violations may also constitute violations of federal, state, or local law and may be referred to appropriate law enforcement authorities.

11.2. Range of Sanctions

11.2.1. Sanctions may include, but are not limited to:

11.2.1.1. Informal warning or reprimand;

11.2.1.2. Mandatory training;

11.2.1.3. Temporary or permanent loss of computing or network privileges;

11.2.1.4. Disciplinary probation;

11.2.1.5. Suspension or dismissal from employment or enrollment;

11.2.1.6. Financial restitution for damages;

11.2.1.7. Referral for criminal prosecution where applicable.

11.3. Temporary Suspension of Access

Access restrictions may be applied in whole or in part and may be limited to specific systems or services, depending on the nature and scope of the risk identified.

11.3.1. The University may temporarily suspend or restrict computing or network privileges when there is reasonable cause to believe that continued access presents a risk to institutional systems, data, operations, or community safety.

11.3.2. Temporary suspension is a protective measure intended to prevent further potential misuse and does not, by itself, constitute a finding of misconduct.

11.3.3. Access may remain restricted during the pendency of an investigation.

11.4. Investigation and Due Process

11.4.1. Alleged violations will be reviewed and investigated by appropriate University officials in coordination with Technology Services, Human Resources, Student Affairs, Academic Affairs, or other relevant offices as appropriate.

11.4.2. Minor or inadvertent violations may be addressed through informal resolution when appropriate. More serious or repeated violations will be addressed through formal disciplinary processes consistent with applicable University policies.

11.4.3. This procedure is not intended to be exhaustive. Conduct not specifically listed but determined to be inconsistent with the spirit or intent of this policy may also be subject to disciplinary action.

12. Policy Review

The Chief Information Officer (CIO), in coordination with Technology Services and Legal Counsel, is responsible for the oversight and maintenance of this policy and associated procedures.

12.1. Review Cycle

12.1.1. This policy and procedures will be reviewed at least annually to ensure alignment with applicable laws, regulatory requirements, cybersecurity standards, and institutional practices.

12.1.2. Interim updates may be made as necessary to address emerging security risks, legal changes, audit findings, or operational requirements.

12.2. Approval and Revision Authority

12.2.1. Substantive revisions to this policy and procedures must be approved in accordance with University governance processes.

12.2.2. The CIO or designee is authorized to implement technical or administrative updates that do not materially alter the intent of the policy but are necessary to maintain security and compliance.

Cross References

1. Doane University Information Security Policy
2. Doane University Acceptable Use of Information Systems and Technology Policy
3. Information Security Procedures
4. Data Governance Standards
5. Technology Procurement and Lifecycle Procedures
6. IA Policy (Work in progress)