UTDBP3096 - Information Security and Accept

capable of creating, storing, or processing University Data.

OIT: Office of Information Technology is the UT Dallas department, led by the Chief Information Officer, assigned responsibility for planning and ongoing operation of centrally-provided information systems such as telecommunications networks, computers, software, databases, system integration and hosted solutions.

Public Data: The subset of University Data intended for public consumption (e.g. marketing materials, press releases, public websites, published papers, and/or UT Dallas-issued email address).

University Data: This Policy uses the term University Data to refer to data for which UT Dallas has a responsibility for ensuring appropriate information security or would be liable for data exposure, as defined by applicable law, UT System policy, regulations, or contractual agreements. University Data may include information held on behalf of UT Dallas or created as a result and/or in support of UT Dallas business (e.g. financial records, personnel records, officially maintained student records, and/or records of official UT Dallas committees), including paper records. This definition does not imply, address, or change intellectual property ownership.

User: Any individual granted access to UT Dallas Information Systems, including guests and contractors.

UT System: The University of Texas System

UT Dallas: The University of Texas at Dallas (also referred to as UTD)

UT Dallas Information Systems: All computer and telecommunications equipment, software, data, and media, owned or controlled by UT Dallas or maintained on its behalf.

Back to Top

Intellectual Property Ownership

This Policy does not create or supersede any existing ownership rights to intellectual property. Existing intellectual property ownership rights defined by applicable law, UT System policy, regulations, or contractual agreements do not change based on storage location. UT Dallas personnel who may have access to content in the course of performing job responsibilities do not obtain ownership rights to that content.

Back to Top

Roles & Responsibilities

Appropriate levels of information security can only be achieved with a well-coordinated team effort across the UT Dallas organization. Stakeholders must work together to identify risks and take responsibility for appropriate controls.

ISO:

Information Security Coordinator (ISC): An ISC is an individual typically designated by a dean or department head to serve as a liaison between the ISO and the DOs.

Data Custodian (DC): The DC is designated by the DO and assists with the ongoing operational tasks of managing

		possible risk to University Data is initiated • UT Dallas has no interest in personally owned data, though personally owned data may be visible to UT Dallas personnel in the course of performing an investigation • Users are discouraged from placing University Data onto personally owned computing devices
Personally owned Data	• In scope for this Policy • ISO, OIT, and/or Decentralized IT may have visibility in the course of performing job responsibilities – Users have no expectation of privacy • UT Dallas has no interest in personally owned data and existing ownership rights remain unchanged • With the exception of personally owned data related to a User's job responsibilities (e.g. scholarly works), Users are discouraged from placing personally owned data onto UT Dallas Information Systems	• Out of scope for this Policy • ISO has no monitoring capability, nor intent to pursue such capability – Users do have expectation of privacy, provided that University Data is not present • UT Dallas has no interest in personally owned data

Users shall never use UT Dallas Information Systems to deprive access to individuals otherwise entitled to access

Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited unless such use is approved by the User's dean or department head.

Incidental Use of UT Dallas Information Systems that directly results in financial gain to the individual – such as work in support of outside employment or self-employment – is prohibited unless such use is approved by the User's dean or department head in accordance with UTDPP1100, "Conflicts of Interest and Conflicts of Commitment."

Incidental Use for purposes of political lobbying or campaigning is prohibited.

Accessing, creating, storing, or transmitting sexually explicit materials during Incidental Use is prohibited. Questions regarding whether particular content is "sexually explicit material" should be directed to UT Dallas counsel or the UT System Office of General Counsel.

Back to Top

Email

Emails sent or received by Users in the course of conducting UT Dallas business are University Data that are subject to state records retention and security requirements.

Users are expected to use UT Dallas-provided email accounts for conducting UT Dallas business, rather than personal email accounts; Users are encouraged to use personal email accounts for conducting personal communication and business, rather than UT Dallas-provided email accounts.

Emails containing Confidential Data must be encrypted with tools and processes approved by the ISO in order to reduce risk of interception.

The following email activities are prohibited when using a UT Dallas-provided email account:

1. Sending an email under another individual's name or email address, except when authorized to do so by the intended User of the email account for a work-related purpose.
2. Accessing the content of another User's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of UT Dallas.
3. Maliciously sending or forwarding any email that is suspected by the User to contain computer malware. Forwarding to a malware researcher or the ISO for analysis does not represent malicious intent.
4. Any Incidental Use prohibited by this policy.
5. Any use prohibited by applicable UT Dallas or UT System policy.

Back to Top

Portable and Remote Computing

All electronic devices including personally owned computing devices used to access, create or store Confidential Data or Controlled Data must be protected by mechanisms (e.g. passwords or biometrics) that limit access to authorized Users, in accordance with UT Dallas Information Security Standards.

UT Dallas-issued mobile computing devices must be encrypted.

Any personally owned computing devices on which Confidential Data is stored or created must be encrypted in a manner which protects the Confidential Data from unauthorized access.

University Data created and/or stored on personal computers, other computing devices and/or non-UT Dallas Information Systems should be transferred to UT Dallas Information Systems as soon as feasible.

Because portable computers, smart phones, and other computing devices are targets for theft, Users are expected to take reasonable precautions to physically secure UT Dallas Information Systems or personally owned computing devices containing University Data when theft is likely (e.g. place inside vehicle trunk when traveling, don't leave unattended at a coffee shop or food court, and/or lock in hotel safe when provided).

All remote access to Confidential Data and Controlled Data must be accomplished using an encrypted method approved by the ISO (e.g. VPN, SSH, and/or Outlook Web Access).

Back to Top

Access Control

Each individual provided with a system account shall maintain securely and never disclose his/her account password or credentials or knowingly permit another individual to access UT Dallas Information Systems via his/her account, except in accordance with a lawful investigation. Any individual who knowingly accesses UT Dallas Information Systems with a user account not specifically assigned to him/her is in violation of this Policy. Similarly, Users may not share individually-assigned access control devices (e.g. Comet Cards, hardware tokens, and/or door keys) unless necessary to preserve life safety.

Computing accounts will be assigned to individuals, except when a shared account is justified by the functions being performed. Accounts designed specifically for a shared purpose or specific system task, such as facilitating data backups or scheduled batch processing, will be granted only in cases when absolutely necessary and will be shared with as few individuals necessary to effectively perform UT Dallas operations.

Computing accounts providing access to UT Dallas Information Systems will only be created when necessary to achieve UT Dallas objectives. Access privileges will be assigned to provide the minimum necessary permission to perform job responsibilities.

UT Dallas Information Systems are subject to risk-based authentication configuration settings defined in Information Security Standards (e.g. password length, complexity, and 2-factor authentication).

Account credentials should not be hard coded into scripts, software code, or system configurations. When hard coding credentials is deemed necessary, system owners will store these files in a secure manner and will maintain sufficient documentation to allow periodic manual changes to passwords or other credentials.

The ISO will administer an annual account sponsorship renewal process, whereby accounts will be verified by responsible management and disabled if no longer necessary or associated with a valid User at UT Dallas.

When employment relationships are subject to change or termination, responsible management will participate in checkout processes defined by Human Resources to ensure timely disabling of system access.

In order to limit the possibility of malicious access, the ISO may disable computing accounts based on reasonable indication that the account has been disclosed to, or compromised by, a malicious third party. The ISO shall assist in re-establishing control of the account by the intended User.

UT Dallas Information Systems access should be designed to maintain separation of duties to reduce the risk of a malicious individual performing conflicting activities (e.g. requesting system access while also approving one's own system access). Compensating controls such as log monitoring and system-enforced thresholds may also be implemented when conflicting duties cannot be separated.

Back to Top

Computer Systems Security

All UT Dallas Information Systems, including production and non-production systems, must be configured and operated in accordance with Information Security Standards.

All UT Dallas Information Systems should be updated with the latest compatible software patches. This includes patches for the operating system and third-party applications. High-priority patches may need to be installed outside of routine change control procedures at the request of the ISO in order to address critical security vulnerabilities.

The ISO may participate at key steps of projects involving access to Confidential Data or Controlled Data. The ISO should assess security controls and notify stakeholders of risks prior to introducing new solutions into production. Costs of security testing, if applicable, will be considered part of the project budget.

All software used at UT Dallas, including commercial and open source, must be used in compliance with End User

Back to Top

Physical Security

Locations that support access to UT Dallas Information Systems must be protected in accordance with value of the information assets at risk. High-risk locations include, but are not limited to, data centers, server closets, wiring closets, file rooms, and research labs.

Users are encouraged to wear UT Dallas identification in restricted access areas; visible UT Dallas identification may be required at the discretion of a dean or department head.

Users who work in restricted access areas should remain aware of unidentified individuals who may attempt to gain access.

Locked doors protecting restricted access areas should not be propped open if unattended.

Users will maintain a workspace where Confidential Data or Controlled Data is stored in a manner to mitigate risk of observation or theft by unauthorized parties (e.g. locked offices, locked file cabinets, and/or privacy screens).

Back to Top

Third-Party Vendors

All third-party vendors that host or access University Data are subject to assessment by the ISO.

Contracts with third parties will include expectations for information security.

Third parties will be expected to protect UT Dallas Information Systems and University Data with security equal to or better than levels defined in this Policy and applicable Information Security Standards.

All third parties performing tasks or data processing for UT Dallas are required to notify UT Dallas immediately if a security incident has occurred, or is suspected to have occurred.

Back to Top

Business Continuity Planning

Individuals responsible for critical operations must maintain a business continuity plan which accounts for facilities, equipment, staffing, and UT Dallas Information Systems needs.

Back to Top

Exemptions

Compliance with all elements of this policy may not be possible in some situations given the tradeoffs between risk, cost, and operational impact. Users may request exemptions to elements of this Policy; requests will be subject to approval or denial by the ISO within 30 days of the request. When applicable, DOs will be asked to accept risks associated with non-compliance. Exemption requests should include an explanation of why compliance with specific Policy elements is not feasible and should describe compensating controls that are in place to reduce risk. Approved exemptions will include an expiration date and be tracked by the ISO.

Exemption requests not approved by the ISO may be appealed to UT Dallas's President.

Back to Top

Disciplinary Actions

Instances of noncompliance, or attempted noncompliance, may constitute a security violation that is subject to investigation and possible disciplinary action, civil prosecution, and/or criminal prosecution in accordance with applicable policies and laws.

Violations may result in disciplinary action by Human Resources in accordance with pertinent policies, up to and including termination of work relationships. Students involved in violations will be referred to the Office of Student Affairs. Suspected illegal activities will be escalated to appropriate law enforcement agencies.

This Policy does not create or supersede any existing UT Dallas processes for taking disciplinary action. The ISO, which shall not take direct disciplinary action against a User, will participate in existing UT Dallas processes for taking disciplinary action.

Server and application administrators may be called upon to provide information to support a disciplinary investigation or similar purpose. Accessing emails, logfiles, or other data for investigative purposes (not to be confused with routine operations, troubleshooting, and system management) without proper authorization – particularly in retaliation for whistleblower complaints – is an actionable abuse of privilege. An authorization matrix is posted at the ISO website as, "Procedures for obtaining access to user data."

Back to Top

Acceptable Use

Per UTS-165, all institutions within UT System must have an Acceptable Use Policy. By acknowledging this Information Security and Acceptable Use Policy, users are acknowledging policies for Acceptable Use.

Back to Top

User Acknowledgement

Users must acknowledge that they received and read the Information Security and Acceptable Use Policy. They must understand and agree that use of UT Dallas Information Systems is conditional upon agreement to comply; noncompliance may result in disciplinary action as outlined above.

Back to Top

Related Links

Texas Administrative Code 202 (TAC 202)
University of Texas System 165 (UTS-165)
Texas Medical Records Privacy Act
Texas Public Information Act
Family Educational Rights and Privacy Act (FERPA)
Health Insurance Portability and Accountability Act (HIPAA)
Payment Card Industry Data Security Standard (PCI DSS)
Gramm–Leach–Bliley Act (GLBA)
Digital Millennium Copyright Act (DMCA)
UT Dallas Records Retention Schedule
Criminal Justice Information Services (CJIS) Security Policy

Policy History

- Issued: 2015-01-22
- Revised: 2016-06-02
- Editorial Amendments: 2018-01-19
- Editorial Amendments: 2019-02-19

Policy Links

- Permalink for this policy: https://policy.utdallas.edu/utdbp3096
- Link to PDF version: https://policy.utdallas.edu/pdf/utdbp3096
- Link to printable version: https://policy.utdallas.edu/print/utdbp3096