UNIVERSITY OF
TEXAS
ARLINGTON

IT-PO-03

Information Security and Acceptable Use Policy

Contents

I. Title

Information Security and Acceptable Use Policy

II. Policy

It is the policy of The University of Texas at Arlington (UTA or University) to protect University Information Resources based on risk against accidental or unauthorized access, disclosure, modification, or destruction and assure the availability, confidentiality, and integrity of these resources while avoiding creation of unjustified obstacles to conducting business and achieving UTA's mission. All individuals granted access to, or use of University Information Resources must be aware of and agree to abide by the following acceptable use requirements. Users must acknowledge the terms of this policy at least annually.

UTA is responsible for the enforcement of information security requirements set forth by federal and state regulations, UT System policies, and contractual obligations. The standards by which the University must demonstrate compliance include, but are not limited to, Texas Administrative Code, Chapter 202 *Information Security Standards* (Tex. Admin. Code § 202), UT System Policy UTS 165 *Information Resources and Security Policy,* and the Family Educational Rights and Privacy Act (FERPA).

A. Roles and Responsibilities

The following roles were established to help ensure risks to University Information Resources are appropriately managed.

1. **Chief Information Officer (CIO)**

   The CIO is responsible for implementing security controls in accordance with the institutional information security program. This role can also be referred to as the Information Resource Manager (IRM).

2. **Chief Information Security Officer (CISO)**

   The CISO is responsible for the implementation and management of the University's Information Security program.

3. **Information Resource Owner (IRO)**

   The IRO is accountable for the security and compliance of information resources and data under their purview. This role at UTA is generally held by VP's and Department Heads.

4. **Information Security Administrator (ISA)**

   The ISA is an individual delegated by an IRO to advocate for the security and compliance of information resources in their respective departments. The ISA is also a member of the ISO working group.

5. **Information Resource Custodian (IRC)**

   The IRC will be responsible for the implementation of security controls and compliance requirements for Information Resources in their respective departments.

6. **User**

   All University employees, including student employees, affiliates, volunteers, or individuals who are otherwise serving as an agent or are working on behalf of the University, must formally acknowledge and comply with the Institution's Acceptable Use Policy.

B. General

1. University Information Resources are provided for the purpose of conducting University and/or System business. However, Users are permitted to use University Information Resources for use that is incidental to the User's official University duties (Incidental Use) as permitted by this policy.

2. Users have no expectation of privacy regarding any University Data residing on University owned computers, servers, or other information resources owned by, or held on behalf of UTA. The

University may access and monitor its Information Resources for any purpose consistent with the University's duties and/or mission without notice.

3. Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the University Data was placed on the personal device.

4. Users may not use University Information Resources to deprive access to individuals otherwise entitled to access University Information, to circumvent University computer security measures; or, in any way that is contrary to the University's mission or applicable law.

5. Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User's official duties as an employee of University and is approved in writing by the employees Vice President. Viewing, access to, or storage or transmission of sexually explicit materials as Incidental Use is prohibited.

6. Users must clearly convey that the contents of any email messages or social media posts that are the result of Incidental Use are not provided on behalf of the University and do not express the opinion or position of University. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas Arlington."

7. Users should report misuse of University Information Resources or violations of this policy to their supervisors or the Information Security Office.

8. All Users must comply with applicable University and System Information Resources Use and Security policies at all times.

C. Data Classification

1. All Information Resource owners, or designated custodians, are responsible for classifying digital data processed by systems under their purview based on sensitivity and risk to ensure the appropriate application of security controls. The classification labels are:

a. Confidential

Information (or Data) is classified as Confidential if it must be protected from unauthorized disclosure or public release based on State or Federal law or regulation, and by applicable legal agreement to the extent permitted by law.

b. **Controlled**

The Controlled classification applies to Information/Data that is not generally created for or made available for public consumption, but may be subject to release to the public through request via the Texas Public Information Act or similar State or Federal law.

c. **Public**

Published Information/Data includes all Data made available to the public through posting to public websites, distribution through email, social media, print publications, or other media.

D. Generative Artificial Intelligence Tools (GenAI Tools)

The use of generative artificial intelligence tools, including but not limited to, ChatGPT, Bard, and DALL-E (collectively "GenAI Tools"), has increased significantly in recent years and these GenAI Tools are being utilized by many different educational institutions to help fulfill business, research, and academic functions. While UTA continues to explore the ways in which GenAI can help it achieve its vision and mission, employees and students must adhere to the following in regards to GenAI use.

1. Allowable Use

a. GenAI Tools may be used with data that is publicly available or defined as Public by UTA's *Data Classification Standard*.

b. In all cases, GenAI Tools use must be consistent with this policy and its associated Standards.

c. Consistent with this policy, faculty should state in the course syllabus any allowed or limited use of GenAI Tools within the course.

d. Any use of GenAI Tools installed on a computer controlled by UTA or under a vendor contract that specifically protects University data and its use in the AI model may be designated as a permittable tool for use with non-public data classifications in accordance with this policy and its associated Standards.

2. Prohibited Use

a. In general, student records subject to FERPA, health information, proprietary information, and any other information classified as Confidential or Controlled under UTA's *Data*

Classification Standards must not be used within public AI models.

b. GenAI Tools of any sort cannot be used for any activity that would be illegal, unethical, fraudulent or violate any state or federal law or UTA or UT System policies.

E. Confidentiality and Security of Data

1. Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing University data in accordance with UTA Policy GA-LA-PO-02 *Records Management & Retention* and Records Management Guidelines.

2. Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official University duties.

3. Whenever feasible, Users shall store Confidential Information or other information essential to the mission of University on a centrally managed server or University sanctioned cloud storage, rather than a local hard drive or portable device.

4. In cases when a User must create or store Confidential or essential University Data on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, the User must ensure the data is encrypted in accordance with University, System's and any other applicable requirements.

5. The following University Data must be encrypted during transmission over an unsecured network: Social Security Numbers; personally identifiable Medical and Medical Payment information; Driver's License Numbers and other government issued identification numbers; Education Records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other University Data about an individual likely to expose the individual to identity theft. Email sent to and received from System and UT System institutions using University and/or System provided email accounts is automatically encrypted. The Office of Information Technology (or other applicable office) will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations.

6. Users who store University Data using commercial cloud services must use services provided or sanctioned by University, rather than personally obtained cloud services.

F. Computer Systems Security

1. All University Information Resources, including production and non-production systems, must be configured in accordance with UTA policies and standards, applicable laws, and requirements of UT System Policy UTS 165 *Information Resources and Security Policy*.

2. Users must not use security programs or utilities except as such programs are required to perform their official duties on behalf of University.

3. All computers connecting to the University's network, must run security software prescribed by the Information Security Officer as necessary to properly secure University Resources.

4. All UTA owned endpoint computing devices will be managed by a centralized Endpoint Management solution to ensure required security controls are enforced.

5. UTA may access and monitor its Information Resources for any purpose consisted with University's duties and/or mission without notice.

6. All UTA Information Resources must be updated to the latest compatible software patches.

7. Networking devices such as routers, hubs, switches, firewalls, and access points may not be attached to the University network without approval from the Director of OIT Infrastructure and Operations.

8. Software that is unlicensed or harmful may be removed from UTA Information Resources at the direction of the CISO.

9. Devices determined by the University to lack required security software or to otherwise pose a threat to University Information Resources may be immediately disconnected by the University from a University network without notice.

G. Email

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

2. Users are to use University provided email accounts, rather than personal email accounts, for conducting University business. Users should not forward University email containing University business to a personal email account.

3. The following email activities are prohibited when using a University provided email account:

   a. Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose.

   b. Accessing the content of another User's email account except:

      i. As part of an authorized investigation;

      ii. As part of an approved monitoring process; or

      iii. For other purposes specifically associated with the User's official duties on behalf of University.

   c. Sending or forwarding any email that is suspected by the User to contain computer viruses except when reporting it to spam@uta.edu.

   d. Any Incidental Use prohibited by this policy.

   e. Any use prohibited by applicable University or System policy.

H. Incidental Use of Information Resources

1. Incidental Use of University Information Resources must not interfere with User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or System policy.

2. Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including University email accounts.

3. A User’s incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located.

4. Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited.

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

6. Storage of any email messages, voice messages, files, or documents created as Incidental Use by a User must be nominal (less than 5% of a User's allocated mailbox space).

7. Files not related to UTA or System business may not be stored on network file servers.

I. Additional Requirements for Portable and Remote Computing

1. All electronic devices including personal computers, smart phones or other devices used to access, create or store University Information Resources, including email, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.

2. University Data created or stored on a User's personal computers, smart phones or other devices, or in data bases that are not part of University's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources.

3. University issued mobile computing devices must be encrypted.

4. Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted.

5. University Data created and/or stored on personal computers, other devices and/or non-University data bases should be transferred to University Information Resources or University sanctioned cloud storage locations as soon as feasible. Confidential University data may not be stored in personal cloud storage accounts. Storing or accessing confidential University information on a jailbroken device (an iOS device which has software restrictions removed) is prohibited.

6. Unattended portable computers, smart phones and other computing devices must be physically secured.

7. All remote access to networks owned or managed by University or System must be accomplished using a remote access method approved by the University or System, as applicable.

J. Password Management

1. University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (*i.e.* Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.

2. Each User is responsible for all activities conducted using the User's password or other credentials.

3. Users must not use the same username and password combination that is implemented on a UTA Information Resource on non-UTA applications or systems.

K. Access Management

1. All users with access to UTA's Information Resources will be provided an individual, unique user account. Users shall never disclose their password or knowingly permit another user to access UTA resources with their account.

2. Access privileges for users will be assigned and maintained with the minimum necessary permission to perform job responsibilities.

3. UTA system access should maintain separation of duties to reduce the risk of malicious activity or conflicts of interest. Where conflicting duties cannot be separated additional oversight or mitigating controls are required.

4. UTA information resources are subject to risk-based authentication settings defined in information security standards published by the Information Security Office (*e.g.* password length, complexity, 2 factor authentication).

5. The CISO may authorize the disabling of computing accounts based on reasonable suspicion that the account has been disclosed or compromised by a malicious third party.

L. Risk Management

1. Information Resource Owners (IRO) in collaboration with the Information Security Office must ensure an annual risk assessment is performed on all Mission Critical Information Resources and Information Resources containing confidential data.

2. The Institutional ISO or delegate must review and approve security requirements, specifications, for any new software, applications or

services that are mission critical or that receive, maintain, and/or share confidential data.

3. Acceptance of high residual risk must be approved by the President, or their designee and documented by the Information Security Office.

M. Third-Party Vendors, Cloud Services, and Software Related Purchases

1. Users who store University Data using commercial cloud services must use services provided or sanctioned by the University, rather than personally obtained cloud services.

2. All third-party vendors or cloud services that host or access University Data are subject to an assessment by the Information Security Office.

3. Third-party vendors or cloud services are expected to meet or exceed UTA's minimum-security policies and standards.

N. Backup and Recovery

1. Data owners should store University data using UTA sanctioned commercial cloud services or a UTA data center to ensure University data will be backed up. Otherwise, the data owner is responsible to ensure University data is backed up.

2. Backups should be tested periodically to ensure functionality.

3. All backup media stored outside of a UTA sanctioned commercial cloud service or UTA data center must be encrypted.

O. Data Destruction

1. Data must be retained according to the UTA data retention schedule. University data no longer needed must be destroyed according to information security standards published by the Information Security Office.

2. Storage media must be securely overwritten prior to reuse and physically destroyed before removing from service.

3. Paper and CD/DVD media must be securely shredded to prevent reassembly.

P. Security Incidents

1. Information Resources Owners, Custodians, and any supervisor or manager who becomes aware of a security incident is to report the incident to the CISO.

2. If a user suspects their University account or computing device has been compromised, please report to the Office of Information Technology (OIT) helpdesk immediately.

Q. Exceptions

1. Exception to an otherwise required security control may be granted by the Information Security Office (ISO) to address specific circumstances or business needs relating to an individual program or department, only as authorized by application law, System and University Policy.

2. All granted exceptions are subject to review and revocation at any time by the ISO as required to maintain, adapt to, or otherwise support the University's security posture.

3. Exception requests not approved by the ISO may be appealed to the President or designee.

R. Violations and Enforcement

1. Violations of the University's Information Resources Acceptable Use and Security Policy are subject to investigation and may be referred to Human Resources or Student Affairs for disciplinary action, civil prosecution, and/or criminal prosecution as permitted by law.

2. UTA reserves the right to administer, reimage, or otherwise secure University information resources when needed. Information resources which do not meet and maintain the minimum standards of compliance set forth by the Information Security Department and pose a serious security threat will be removed from the network and isolated until remediation or mitigating controls can be validated by the CISO or designee.

S. Prohibited Technologies

1. On January 26, 2023, the Texas Department of Information Resources (DIR) issued a Model Security Plan (Plan) for Prohibited Technologies applicable to all Texas state agencies and institution of higher education. The Plan is intended to protect sensitive information and critical infrastructure from technology that poses a threat to the State of Texas. UTA endeavors to comply with this Plan and UTA's Information Security Office has published a Prohibited

Technologies Security Policy as part of their required policies and standards. The policy link is found in Section V of this policy.

III. Definitions

Cloud Services: A service that provides network access to a shared pool of configurable computing resources on demand that may be rapidly provisioned and released by the service provider with minimal effort or interaction.

Confidential Data or Confidential Information: All University Data that is required to be maintained as private or confidential by applicable law.

Controlled Data: University data that is not generally made available for public consumption but may be subject to release under the Texas Public Information Act or other laws.

Information Security Program: The policies, standards, procedures, strategies, objectives, plans, metrics, reports, resources and services adopted for the purpose of securing University Information Resources.

Information Security Officer (ISO): The Information Security Office at UTA, led by the Chief Information Security Officer, is responsible for the University's information security program.

Mission Critical Information Resource: Information Resources defined by an institution to be essential to the institution's ability to meet its instructional, research or public services.

Office of Information Technology (OIT): Office of Information Technology at UTA, led by the Chief Information Officer, is responsible for planning and the ongoing operation of centrally provided technology services.

Public Data: University data that is intended for public consumption (*e.g.* marketing materials, press releases, public websites).

System: The University of Texas System

University: The University of Texas at Arlington

University Data: All data or information held on behalf of the University, created as result and/or in support of University business, or residing on University Information Resources, including paper records.

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

IV. Relevant Federal and State Statutes

Family Educational Rights and Privacy Act, 34 C.F.R. Part 99

Texas Administrative Code, Title 1 Administration, Part 10 Department of Information Resources, Chapter 202 *Information Security Standards*

V. Relevant UT System Policies, Procedures and Forms

UTA Policy GA-LA-PO-02 *Records Management & Retention*

UT System Policy UTS 165 *Information Resources and Security Policy*

Information Security Office Policies and Standards:

- Approved Data Storage
- Information Security Procedures for Procurement of Software and Cloud-Based Services
- Information Security Risk Management Program Standard
- Minimum Server Security and Hardening Standards
- Password Security
- Secure Media Destruction
- Prohibited Technologies Security Standard

VI. Who Should Know

All individuals granted access to or use of UTA information resources.

VII. UTA Office(s) Responsible for Policy

Responsible Officer: Chief Information Officer

Sponsoring Department: Information Security Office

VIII. Dates Approved or Amended

April 13, 2015

July 13, 2021

May 9, 2022

February 15, 2023

July 16, 2024

IX. Contact Information

All questions regarding this policy should be directed to the Information Security Office: security@uta.edu

Send notifications of errors or changes to: policysite@uta.edu