# UTAH TRANSIT AUTHORITY POLICY

## UTA.01.20

## INFORMATION SECURITY

1) Purpose

This policy establishes the minimum requirements, ethics, responsibilities and accepted behaviors required to protect and maintain confidentiality, integrity, and availability of information and related Information Technology Resources. This policy acts as an umbrella policy, which seeks to establish and maintain a secure environment for Utah Transit Authority's (UTA's) information based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This policy is applicable to all UTA employees and non-UTA employees, including outsourced third parties, who have access to or who manage UTA information and information technology. This policy acts as an umbrella document to all other security policies and associated standards. It encompasses all electronic systems, automated and manual, for which UTA has administrative responsibility, including systems managed or hosted by third parties on behalf of UTA. It is applicable to all information, regardless of the form or format, which is created or used in support of business activities at UTA.

2) Definitions

*"Agency Access Control Standard"* means the Agency's formally adopted standard that prescribes requirements for the authorization, provisioning, management, monitoring, and revocation of access to Agency information systems, data, and assets, based on least privilege and business need, and in compliance with applicable law and Agency policy.

*"Authentication Token"* means a mechanism to prove the identity of a user electronically, to include User name, password and badge number.

*"Authorized User"* means any User who is authorized to use a specific Technology Resource. Authorization may be based on job titles, job roles, or other methods of access control. Authorization will be determined by the Technology Department in consultation with the data owner.

*"Cardholder Data"* means the card number, as defined by PCI-DSS, that identifies the issuer and the particular cardholder account by itself or in conjunction with the cardholder's name, expiration date, cardholder address, cardholder social security number or any other type of cardholder identifying information. Cardholder Data applies to data stored on hard-copy media (such as reports and receipts), electronic media (such as computers, hard drives, Portable Devices), and stored in databases or in transaction logs.

*"Compensating Control"* means any data security measure that is designed to satisfy the requirement for some other security measure that is deemed too difficult or impractical to implement. A Compensating Control must provide a similar level of defense to comply with any legal, regulatory or contractual requirements.

*"Executive Team"* means the group of senior organizational leaders who are authorized to make strategic decisions regarding data governance, risk management, and information security. The

Executive Team is responsible for approving safeguards, policies, and procedures related to the handling of PII, and may delegate specific responsibilities to designated officers or committees as appropriate.

*"GRAMA"* means the Utah Governmental Records Access and Management Act codified at Utah Code Ann.§ 63G-2-101 et seq.

*"Information Security Officer"* or *"ISO"* or *"Information Security Representative"* means the individual accountable for the duties and functional responsibilities listed in Section 3.A.2.

*"IT Director"* means the senior official responsible for overseeing the organization's information technology strategy, infrastructure, and operations, and who is accountable for ensuring the confidentiality, integrity, and availability of information systems and data, and for implementing and maintaining appropriate security controls.

*"NIST CSF"* refers to the National Institute of Standards and Technology (NIST Cybersecurity Framework (CSF). The NIST CSF provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks.

*"Non-Disclosure Agreement"* or *"NDA"* means a legal contract that outlines how to protect and use confidential information shared between two or more parties.

*"Payment Card Industry Data Security Standards"* or *"PCI-DSS"* means data security standards developed by the major payment card companies (Visa, MasterCard, Discover, and American Express) as a guideline to help organizations that process card payments prevent fraud, hacking, and various other security vulnerabilities and threats.

*"Personal Identifying Information"* or *"PII"* means any data that can be used to identify, contact, or locate a single individual, either directly or indirectly. PII includes both sensitive and non-sensitive information and may exist in physical or electronic form. PII includes, but is not limited to: (i) full name, (ii) home or mailing address, (iii) email address, (iv) telephone number, (v) social security number, (vi) driver's license or state identification number, (vii) passport number, (viii) financial account numbers (e.g., bank account, credit card, etc.), (ix) date and place of birth, (x) biometric identifiers (e.g., fingerprints, facial recognition data, etc.), (xi) medical, health, or insurance information, (xii) employment or educational records, (xiii) login credentials (e.g., usernames and passwords), and (xiv) IP addresses or device identifiers when linked to an individual. Sensitive PII is information that, if compromised, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Non-sensitive PII may be publicly available but can still be considered PII when combined with other data elements that enable identification. All personnel must handle PII in accordance with applicable laws, regulations, and organizational standards to ensure its confidentiality, integrity, and availability.

*"Portable Devices"* include, but are not limited to, any laptops, PDAs, smartphones, and other removable storage devices such as flash (thumb) drives.

*"Recovery Point Objective"* or *"RPO"* means the maximum acceptable amount of data loss measured in time. It defines the point in time to which data must be restored following a disruption, indicating how much data can be lost without causing unacceptable harm to the organization.

*"Recovery Time Objective"* or *"RTO"* means the maximum acceptable amount of time that a system, application, or process can be unavailable after a disruption before causing significant impact to business operations. It defines the target duration for restoring functionality following an incident.

*"Security Incident"* means any activity that harms or represents a serious threat to the whole or part of UTA's Technology Resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software, or data, unauthorized exposure, change or deletion of confidential data, activities contrary to the UTA's corporate policies, or a crime or natural disaster that destroys access to or control of these resources.

*"Sensitive Data"* means any data which has been classified as private, controlled, protected, Sensitive Security Information, or confidential in UTA's Records Access and Management Policy or as designated under federal and state law, policy, or regulation.

*"Suitability Determinations"* may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state, and private sources that maintain public and non-public records. A Suitability Determination must provide reasonable grounds for the entity to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the entity.

*"Technology Resource(s)"* means any desktop, laptop, hardware, software, data, storage media, removable storage media (such as CDs and USB drives), electronic communications devices, networks (including, but not limited to, wired or wireless networks, e-mail, fax, cell phones, audio and digital recordings, phone systems and voice mail), and any cloud solutions such as, but not limited to off-site storage, Software as a Service or Infrastructure as a Service. The term also includes any operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, UTA's shared computing and network infrastructure.

*"Trusted Network"* means any Technology Resource which UTA uses to conduct its internal business and is controlled and protected by the Technology department. The Wi-Fi segment used by personally owned devices is not considered a Trusted Network.

*"Untrusted Network"* means a communication network that is internal or external to the networks belonging to UTA and which is out of UTA's ability to control or manage.

*"Users"* means individuals using UTA's Technology Resources including all full-- and part-time employees and individuals who work under an agreement with UTA such as contractors, consultants, vendors, volunteer, and other persons in similar positions.

3) Policy
   A. Functional Responsibilities
      1. Executive Leadership
         a. Evaluating and accepting risk on behalf of UTA;

b. Identifying information security responsibilities and goals and integrating them into relevant processes;
c. Supporting the consistent implementation of information security policies and standards;
d. Supporting security through clear direction and demonstrated commitment of appropriate resources;
e. Promoting awareness of information security best practices through the regular dissemination of materials provided by the designated ISO/Information Security Representative;
f. implementing the process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;
g. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;
h. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
i. participating in the response to Security Incidents;
j. complying with notification requirements in the event of a breach of private information;
k. adhering to specific legal and regulatory requirements related to information security;
l. communicating legal and regulatory requirements to the ISO/Information Security Representative; and
m. Communicating requirements of this policy and the associated standards, including the consequences of noncompliance, to the workforce and third parties, and addressing adherence in third party agreements.

2. Information Security Officer (ISO)/Information Security Representative
   a. Providing in-house expertise as security consultant as needed;
   b. Developing the security program and strategy, including measures of effectiveness;
   c. Establishing and maintaining agency information security policy and standards;
   d. Assessing compliance with security policies and standards;Advising on secure system engineering (security by design);
   e. Providing incident response coordination and expertise;
   f. Monitoring networks for anomalies;
   g. Monitoring external sources for indications of data breaches, defacements, etc.;
   h. Maintaining ongoing contact with security groups/associations and relevant authorities and regulatory bodies;
   i. Providing timely notification of current threats and vulnerabilities;
   j. Maintaining familiarity with business functions and requirements;
   k. Maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;
   l. Assessing compliance with information security policies and legal and regulatory information security requirements;
   m. Evaluating and understanding information security risks and how to appropriately manage those risks;
   n. Representing and assuring security architecture considerations are addressed;

o. Advising on security issues related to procurement of products and services;
p. Escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
q. Disseminating threat information to appropriate stakeholders;
r. Participating in the response to potential Security Incidents;
s. Participating in the development of enterprise policies and standards that consider UTA's needs; and
t. Promoting information security awareness through awareness materials and training resources.

3. Information Technology Management
   a. Supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;
   b. Limiting User's access to Technology Resources based on best practices, least privilege or contractual, compliance or regulatory requirements;
   c. Providing resources needed to maintain a level of information security control consistent with this policy;
   d. Identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;
   e. Implementing the proper controls for information owned based on the classification designations;
   f. Providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);
   g. Fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures; and
   h. Implementing business continuity and disaster recovery plans.

4. Individual Employees
   a. Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information entrusted;
   b. Protecting information and resources from unauthorized use or disclosure;
   c. Protecting personal, private, sensitive information from unauthorized use or disclosure;
   d. Abiding by the Acceptable Use of Information Technology Resources Policy;
   e. Reporting suspected information Security Incidents or weaknesses to the appropriate manager and ISO/Information Security Representative;
   f. Accessing UTA's Technology Resources through the use of individually assigned unique usernames, or equivalent technologies;
   g. Authenticating with an Authentication Token associated with each username when accessing the data, systems, or networks of UTA;
   h. Accessing only those information assets for which they are authorized;
   i. Reasonably protecting against unauthorized activities performed under their username by never sharing their login or authentication information;
   j. Complying with the Agency Access Control Standard; and
   k. Protecting Authentication Tokens as Sensitive Data while in transit and at rest.

B. Separation of Duties

1. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
2. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails, and management supervision.
3. The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

C. Information Risk Management
1. Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development lifecycle.
2. Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
3. Entities are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.
4. Risk assessment results, and the decisions made based on these results, must be documented.

**Associated Standards: Information Security Risk Management Standard; Secure System Development Lifecycle (SSDLC) Standard**

D. Information Classification and Handling
1. All information, which is created, acquired, or used in support of business activities, must only be used for its intended business purpose.
2. All information assets must have an information owner established within the lines of business.
3. Information must be properly managed from its creation, through authorized use, to proper disposal.
4. All information must be classified on an ongoing basis based on its confidentiality, integrity, and availability characteristics.
5. An information asset must be classified based on the highest level necessitated by its individual data elements.
6. If UTA is unable to determine the confidentiality classification of information or the information is PII the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
7. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.
8. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
9. Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.
10. UTA must communicate the requirements for secure handling of information to its workforce.
11. A written or electronic inventory of all information assets must be maintained.

12. Content made available to the general public must be reviewed according to a process that will be defined and approved by the appropriate department (Marketing, Communications, or Records). The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
13. PPI must not be made available without appropriate safeguards approved by the Executive Team.
14. Before any non-public information is released outside UTA or shared with external entities, a formal process must be established and documented. At a minimum, this process must:
    a. Evaluate, define, and document the sensitivity and classification of the information to be released or shared;
    b. Identify the responsibilities of each party for protecting the information, including legal and regulatory obligations;
    c. Specify and define the minimum technical and administrative controls required for transmission, storage, and use of the information;
    d. Record the existing safeguards and security measures that each party has in place to protect the information;
    e. Define a method for compliance measurement;
    f. Provide a signoff procedure for each party to accept responsibilities; and
    g. Establish a schedule and procedure for periodic review and reassessment of the controls.

**Associated Standards: Information Classification Standard; Sanitization/Secure Disposal Standard**

E. Information Technology Asset Management
1. All IT hardware and software assets must be assigned to a designated business unit or individual.
    a. To obtain Technology Resources, a User must request approval from his or her manager or executive and submit a written request to the IT Director or designee for review and approval.
    b. All UTA owned Technology Resources are controlled by the Technology department and must be surrendered upon request for maintenance, review, or audit.
    c. Access to Technology Resources by contractors will be approved by the contractor's UTA manager, and the contractor must sign an NDA to receive access to UTA Technology Resources.
    d. It is the responsibility of the contractor's UTA manager to inform the Technology Department when access is to be removed.
    e. The Technology department can restrict access to a contractor as it deems appropriate.
2. Entities are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.
3. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

4. All UTA Technology Resources, including the data transmitted or stored by them, are the sole property of UTA. Accordingly, UTA may access and monitor User's communications and files as it considers appropriate, including but not limited to any personal e-mail accounts, files, and text messages accessed on a UTA Technology Resource.
5. Departments within UTA are responsible for physical security for personal computers and other local Technology Resources, including portable equipment, housed within their immediate work area or under their control.
6. All Users are expected to use and handle UTA's physical electronic and intellectual property with care. Users may not use e-mail, instant messaging services, facsimiles, cellular telephones, social media websites or any other communications system to communicate Sensitive Data external to UTA unless authorized. Users must refer individuals requesting any records to UTA's Records Officer as described in UTA's Privacy SOP. The disclosure of restricted records is a Class B Misdemeanor under GRAMA.

**Associated Standard: Secure Configuration Standard**

F. Personnel Security
   1. The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific UTA sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by UTA.
   2. UTA must require its workforce to abide by the Acceptable Use of Information Technology Resources Policy, and an auditable process must be in place for Users to acknowledge that they agree to abide by the policy's requirements.
   3. All job positions must be evaluated by the ISO/Information Security Representative to determine whether the position requires access to sensitive information and/or sensitive information technology assets.
   4. For those job positions requiring access to sensitive information and sensitive information technology assets, UTA must conduct workforce Suitability Determinations upon hire or transfer into such position.
   5. A process must be established within UTA to repeat or review Suitability Determinations periodically and upon change of job duties or position.
   6. All issued property must be returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

**Associated Standard: Account Management/Access Control Standard**

G. Cyber Incident Management
   1. UTA must have an incident response plan and consistent standards to effectively respond to Security Incidents.
   2. All observed or suspected information Security Incidents or weaknesses are to be reported to appropriate management and the ISO/Information Security Representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the ISO directly.

3. The ISO/Information Security Representative must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

**Associated Standard: Cyber Incident Response Standard**

H. Account Management and Access Control
   1. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and Information Technology (IT).
   2. Except as described in UTA's Technology Access Control Standard Operating Procedure, access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs.
   3. Associated with each user-ID is an Authentication Token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.
   4. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.
   5. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.
   6. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.
   7. Tokens must not be stored on paper, or in an electronic file, hand-held device, or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/Information Security Representative.
   8. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).
   9. Access privileges are granted in accordance with the User's job responsibilities and are limited only to those necessary to accomplish assigned tasks in accordance with entity missions and business functions (i.e., least privilege).
   10. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).
   11. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, and that User activities may be monitored and the User should have no expectation of privacy.
   12. Advance approval for any remote access connection must be provided by the entity. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.
   13. All remote connections must be made through managed points-of-entry reviewed by the ISO/Information Security Representative.

14. Working from a remote location must be authorized by management and practices which assure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

**Associated Standards: Account Management/Access Control Standard; Authentication Tokens Standard; Security Logging Standard; VPN Access Agency Standard**

I. Systems Security
   1. Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.
      a. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of the entity. A list of assigned individuals or groups must be centrally maintained.
      b. Security must be considered at system inception and documented as part of the decision to create or modify a system.
      c. All systems must be developed, maintained, and decommissioned in accordance with a secure system development lifecycle (SSDLC).
      d. Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
      e. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
      f. Environments and test plans must be established to validate the system works as intended prior to deployment in production.
      g. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
      h. Formal change control procedures for all systems must be developed, implemented, and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.
         1. Databases and Software (including in-house or third party developed and commercial off the shelf (COTS)):
            a. All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
            b. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.
            c. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:
               1. All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
               2. Sensitive data is masked or overwritten with fictional information.
            d. Where technically feasible, development software and tools must not be maintained on production systems.

e. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
f. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
g. Privileged access to production systems by development staff must be restricted.
h. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

2. Network Systems:
   a. Connections between systems must be authorized by the executive management of all relevant entities and protected by the implementation of appropriate controls.
   b. All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the ISO/Information Security Representative annually, at a minimum, to assure:
      1. The business case for the connection is still valid and the connection is still required; and
      2. The security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.
   c. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
      1. Internet accessible systems and internal systems;
      2. Systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems; and
      3. User and server segments.
   d. Network management must be performed from a secure, dedicated network.
   e. Authentication is required for all Users connecting to internal systems.
   f. Network authentication is required for all devices connecting to internal networks.
   g. Only authorized individuals or business units may capture or monitor network traffic.
   h. A risk assessment must be performed in consultation with the ISO/Information Security Representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

3. External Connections
   a. All connection between UTA's Trusted Networks and any Untrusted Network must be controlled by a firewall and only installed and configured by the Technology department.
   b. All "new" connections from UTA's firewalls to an Untrusted Network must be approved by the IT Director and configurations approved by the Technology Configuration Control Board (TCCB). Subsequent changes to

the configurations are to be approved via the TCCB. The security requirements for each connection must be assessed individually and driven by the business needs of the parties involved. All connections must comply with all regulatory requirements.

c. All connections from UTA's Trusted Network to any Untrusted Network requires strong encryption.
d. Third party connections to a UTA network must have an internal UTA sponsor develop a business case for the network connection. A UTA NDA must be signed by a duly appointed representative from the third-party organization who is legally authorized to sign such an agreement. In addition to the agreement, the third party's equipment must also conform to the UTA's security policies and standards, and be approved for connection by the IT Director, or designee identified via memorandum.
e. Only Authorized Users will be permitted to remotely connect to UTA's computer systems, networks, and data repositories to conduct UTA related business from an Untrusted Network. Such connections must be done through an approved, secure, authenticated, and centrally managed method of remote access.
f. Users who work from a remote location are required to abide by the Technology Access Control Standard Operating Procedureand sign the VPN Access Request Form.

**Associated Standards: Secure System Development Lifecycle Standard; Secure Coding Standard; Security Logging Standard; Secure Configuration Management Standard; VPN Access Agency Standard**

J. Internet Access
1. The Technology department has the obligation to provide/allocate/limit Internet access to provide a balance between accessibility, performance, and security.
2. All Internet traffic via UTA networks (local area network, wireless, or other, whether by a UTA employee or non-UTA employee) is the property of UTA and is subject to review, audit, and access by UTA.

K. Collaborative Computing Devices
1. Collaborative computing devices must:
   a. Prohibit remote activation;
   b. Provide Users physically present at the devices with an explicit indication of use; and
   c. Provide simple methods to physically disconnect collaborative computing devices.

L. Vulnerability Management
1. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.
2. All systems are subject to periodic penetration testing.
3. Penetration tests are required periodically for all critical environments/systems.
4. Where the entity has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing must be coordinated.
5. Scanning/testing and mitigation must be included in third-party agreements.

6. The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/Information Security Representative for evaluation of risk.
7. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.
8. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/Information Security Representative. The ISO/Information Security Representative must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.
9. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested, and followed at all times to minimize the possibility of disruption.

**Associated Standards: Patch Management Standard; Vulnerability Scanning Standard**

M. Operations Security
1. System configurations must follow approved configuration standards.
2. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.
3. Host-based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed.
4. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.
5. Controls must be implemented to disable automatic execution of content from removable media.
6. Controls must be implemented to limit storage of information to authorized locations.
7. Controls must be in place to allow only approved software to run on a system and prevent execution of all other software.
8. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.
9. All security patches must be reviewed, evaluated, and appropriately applied in a timely manner. This process must be automated, where technically possible.
10. Systems which can no longer be supported or patched to current versions must be removed.
11. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard, and record events to provide evidence and to reconstruct lost or damaged data.
12. Audit logs recording exceptions and other security-relevant events must be produced, protected, and kept consistent with record retention schedules and requirements.
13. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound, and internal network traffic.
14. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

15. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly.
16. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers, and other communication equipment).
17. RTOs/RPOs must be established for all critical systems.
18. Backup copies of entity information, software, and system images must be taken regularly in accordance with the entity's defined requirements.
19. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.
20. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

**Associated Standards: Secure Configuration Management Standard; Security Logging Standard; Cyber Incident Response Standard; Account Management/Access Control Standard**

N. Electronic Communication
   1. Incidental use of any Technology Resource to transmit personal messages will be treated no differently than other messages, and may be accessed, reviewed, copied, deleted, or disclosed.
   2. Notwithstanding UTA's right to access any electronic communication, all electronic communications should be treated as confidential by other Users and accessed only by the intended recipient.

O. Portable Devices
   1. No portable device or media may store, process, or transmit Sensitive Data without suitable protective measures that have been approved by the IT Director, or designee.
   2. A User may be allowed to retain possession of a portable Technology Resource during non-work hours. However, in the event of loss or damage to the Technology Resource, the User may be responsible for paying for replacement or repair of the equipment.

P. Application Access Control
   1. Access to UTA's systems applications must be restricted to those individuals who have a business need to access those applications or systems in the performance of their job responsibilities and have approval from the IT Director, or designee and the business owner (manager level or above).
   2. Access to source code for applications and systems must be restricted so that authorized UTA staff and contractors can access only those applications and systems they directly support.

Q. Software Usage
   1. Software may only be used in accordance with any applicable licensing agreement. Copying any UTA owned software without proper authorization may be considered a copyright infringement and is strictly prohibited.
      a. All licensed software acquired for or on behalf of UTA or developed by UTA employees or contractors on behalf of UTA is and at all times will remain UTA

property. Licensed software can only be installed on UTA Technology Resources by the Technology department and must be added to the software inventory system with license information. Staff other than IT installing licensed software can introduce situations where the license information will not be uploaded and tracked appropriately, thus putting UTA at risk.

2. Software can be installed by non-IT staff on UTA Technology Resources with the following conditions: appropriate applications (apps) (non-offending and nothing to cause embarrassment to UTA) on issued smartphones and tablets; and software updates for standalone systems that do not affect UTA operations or information security.
3. All software must protect UTA's Technology Resources from unauthorized disclosure, unauthorized modification, disruption or destruction.
4. Software cannot be used to bypass UTA security controls.
5. Software cannot be installed that violates UTA's corporate or departmental policies.

R. Exceptions
1. Legacy Technology Resources are exempt from this policy if the cost is overly burdensome, or the technology does not exist to secure them. Once a legacy Technology Resource is replaced or upgraded, this exemption no longer applies.
2. Compensating Controls may be implemented to exempt a Technology Resource from this UTA policy. The Compensating Controls must be agreed upon by the business owner and the IT Director. The Compensating Controls must comply with any contractual or regulatory requirements.

S. Improper Use of Technology Resources
1. Improper use of UTA's Technology Resources or any other violations of this policy will result in discipline up to and including termination. Improper use includes any misuse as described in this policy, as well as any misuse that would result in violations of state or federal laws, rules, regulations or other UTA policies.
2. The Technology department has the right to disallow or disconnect any User or device from UTA's Technology Resource without prior consultation.

T. Review of Resource Communications and Files for Investigations and Work-Related Purposes
1. Users have no expectation of privacy related to their usage of UTA-provided computer, hardware, software, or other electronic devices.
2. Users who are responsible for monitoring Technology Resources or who are engaged in data investigations or support are permitted to review resource communications and files as part of their assigned responsibilities and have received approval from the IT Director or ISO/Information Security Representative.
3. No other User is authorized to review any other active User's communications and files residing on UTA's Technology Resources without obtaining the prior express consent of: (1) the IT Director or designee, (2) the general counsel or designee; and (3) the applicable executive of the Executive Team of the subject employee. Such consent will be granted only where there is a non-investigatory work-related purpose for the review and/or an investigation of work-related misconduct. The Manager of Civil Rights Compliance may be advised and consulted regarding the review as deemed appropriate.

4. When and after an employee is separated from UTA (no longer an active employee), in order for the department to provide continuity of operations, the separated employee's email account, personal computer files, and network files can be requested by the manager of the terminated employee to be accessed by another employee but must have the approval of a director or above, and also the IT Director.
5. The prior express consent of the executive director and the general counsel is required to authorize the review of the communications and files of any employee reporting directly to the executive director for a non-investigatory work-related purpose and/or for an investigation of work-related misconduct.

U. Users must immediately report all technical violations of this policy to the Helpdesk or via email to abuse@rideuta.com. Suspected violations involving a User's misuse of Technology Resources or confidential information should be reported to the User's manager, human resources, IT Director, or the Office of Attorney General.

V. In accordance with regulatory and contractual obligations, this policy will be reviewed on an annual basis.

4) Cross-References

- UTA.01.08 Records Access and Management
- AGCY.01.03 Technology Access Control
- Corporate Policy 1.1.24 Acceptable Use of Technology Resources
- § 63G-2-101 et seq. Government Records Access and Management Act (GRAMA)

This UTA Policy was reviewed by UTA's Chief Enterprise Strategy Officer on 03/03/2026 , and approved by the Executive Director on _____. This policy takes effect on the latter date.

_____

Jay Fox
Executive Director

Approved as to form and content:

DocuSigned by:
Mike Bell
70E33A415BA44F6...
Counsel for the Authority

**History**

| Date | Action | Owner |
|---|---|---|
| | Board Reviewed – UTA.01.20 Information Security | Chief Enterprise Strategy Officer |
| | Adopted – UTA.01.20 Information Security | Chief Enterprise Strategy Officer |