Utah Tech University Policy

463 A: University Information Security Rules and Standards

I. Purpose

1.1 Securing Information Technology Resources and Data is a complex and dynamic process. Addendum 463a outlines specific IT Security rules, standards, and practices to be adhered to at Utah Tech University. Due to the constant change of technology and its security risk and threat landscape, the rules, standards, and practices discussed in this document are typically based in principles, not specific systems or products. Where appropriate, the Information Security Office (ISO) and Utah Tech IT Services will maintain records of the current specific applications or practices related to and in accordance with these rules and standards outlined on its publicly accessible web site, found at https://help.utahtech.edu.

II. Definitions

2.1 ***Administrative Rights:*** The privilege or ability of a user to exercise root level control of a computer, system, or other IT resource. This includes but is not limited to the ability to install or remove software, change system settings, create additional users, create, delete, or modify any file, etc.

2.2 ***Information Security Awareness Training:*** Training provided by the University to assist users to understand and recognize current information security threats and risks.

2.3 ***Managed University-owned Device:*** A computer, workstation, or mobile device that is owned by the University and managed centrally by IT Services.

2.4 ***Multi-Factor Authentication:*** An authentication system that requires more than one distinct authentication factor. Multi-Factor Authentication can be performed using a multi-factor authenticator, or by a combination of authenticators, that provides different factors. Typical authentication factors include something you know (a password), something you have (a phone or token), and/or something you are (a biometric, such as a fingerprint).

2.5 ***Network Segmentation:*** The practice of dividing networks into different areas or segments based on function or appropriate security levels. Examples include but are not limited to student networks, employee networks, data center networks, and infrastructure networks.

2.6 ***Remote Access:*** Any means to access University systems, IT resources, or data when not physically located at the University's campuses or physical premises.

2.7 ***University Single Sign-On (SSO):*** A centralized authentication service provided by IT Services that uses the standard Digital ID account.

2.8 ***University Virtual Private Network (VPN):*** A sanctioned and protected remote access system linking to the University's internal network, as provided by University IT Services.

2.9 ***Wireless (Wi-Fi) Networking:*** Technologies and devices that use Radio Frequencies to provide network services.

III. Rules

3.1 **Administrative Rights to University-owned workstations:** University-owned workstations and laptop computers are not distributed to employees with Administrative Rights by default. Granting Administrative Rights is not considered a security best-practice in any industry. While it is convenient for employees to install software without interaction with UT IT Services, or Administrative Rights may be necessary in some cases for an employee to do parts of their job, it also elevates the amount of damage that can be done from a phishing or malware attack. This risk extends to both the computer and other University systems, depending on the employee's data and network level access. Administrative Rights may create opportunities for misuse, such as employees using University-owned computers for extensive non-University-related purposes or allowing their children and/or significant others to do so. It is difficult to defend mere convenience as a good reason to grant Administrative Rights.

3.1.1 University IT Services will implement, as far as possible, technologies, including Privilege Access Management (PAM), to provide University users appropriate permissions to perform their job functions or academic studies without granting full Administrative Rights on University owned and managed devices.

3.1.2 Employees with a business purpose for full Administrative Rights may request these privileges through their supervisors and/or department reporting structure. Supervisors, Data Stewards, and

Data Trustees should weigh the intent and benefit of the request against the risks posed. ISO may be consulted as necessary.

3.1.3 ISO reserves the right to revoke Administrative Rights as necessary to protect University IT resources and data.

3.2 **Managed University-owned Devices**: IT Services maintains a management framework for workstations, laptops, and other computing devices purchased with University funds. A University-owned device is considered managed when it operates within the provided management framework and has appropriate, centralized security controls applied. These controls include, but are not limited to, endpoint protection software, full-disk encryption, privilege access management, and operating system hardening. A properly managed University-owned workstation may be considered an Official IT Resource defined in Policy 463.

3.2.1 Data Trustees, Data Stewards, and/or departments, with an expectation that users under their direction will be working with Controlled Data as part of their essential job functions must provide managed University-owned workstations for these functions to be performed.

3.2.2 Unmanaged devices, regardless of University, third-party, or personal ownership, are not permitted to transmit, store, or otherwise traffic in Controlled Data.

3.2.3 Any exception regarding use of Controlled Data on unmanaged workstations must be approved by an appropriate Data Trustee after review and advisement from ISO on risk to said Controlled Data. Documented compensating controls must be in place.

3.3 **Multi-Factor Authentication (MFA):** To help protect University IT resources, data, and users from access by unauthorized parties, use of Multi-Factor Authentication is required. Any system or resource, whether hosted locally or third-party (cloud or hosted) presenting a public (Internet-facing) login using University Single Sign-On (SSO) or directory credentials must utilize MFA as an additional security control. All employees and active students must be enrolled in the MFA system.

3.3.1 Internal systems or resources should directly leverage MFA where possible, or alternatively, require connection to an MFA-enabled gateway such as the University VPN, before access can be gained to the system or resource.

3.4 **Network Segmentation and Controls:** To protect the internal University network, data, and IT Resources housed thereon, IT Services and the Information Security Office (ISO) have developed a Network Segmentation regime to create network zones of similar function, classification, and/or trust level. Examples of zones or segments include, but are not limited to, student wireless, data center servers, managed staff workstations, etc. These zones are enforced via network firewalls and network access lists.

3.4.1 Principles regarding these segments and zones that IT Services will adhere to include, but are not limited to:

3.4.1.1 Inbound connections from the Internet will be blocked by default at the University perimeter (commonly known as a default-deny stance).

3.4.1.2 University servers or systems providing a network service to the Internet or the University campus at-large must be located in a sanctioned University Data Center segment.

3.4.1.3 Segments of differing trust levels or function will not be mixed and must have firewall controls in place between them.

3.4.1.4 Outbound connections from the University network are generally permitted but are not unlimited. IT Services and the ISO reserve the right to block certain outbound ports, protocols, and applications to reduce security risk to the University and prevent misuse of University network resources.

3.4.2 Exceptions to the above principles may be granted after review and approval by ISO and when appropriate compensating controls are in place.

3.5 **Security Awareness Training:** All University employees must take Information Security training as part of the University's Information Security program. Training will take place at new hire and annually thereafter, typically as part of the University's annual employee training processes. Training materials will be selected at the discretion of the Information Security Office and Human Resources.

3.5.1 Additional training and security exercises such as live phishing training and/or social engineering penetration testing may also be undertaken periodically. These exercises are intended to assess the effectiveness of annual user training courses and the general information security readiness of University employees.

3.6 **Remote Access to internal University Networks:** Uncontrolled, decentralized remote network access to the University network presents significant risks to the security stability of the University network and to Controlled Data stored on University IT Resources. Non-standard Remote Access systems may bypass safeguards and controls designed to protect the University network and data stored on University IT Resources. In addition, commodity or non-standard Remote Access services provided by third parties are not subject to University policies, have no obligation to protect University data, and may not provide audit capabilities to University IT staff and Data Stewards. The University reserves the right to control access to its internal networks and systems. To do so, a sanctioned VPN service will be maintained and offered to the University community and its partners by IT Services. All users including third party contractors or service providers are expected to use this VPN service to gain access to systems or resources that are housed on the University's internal network. Users are not authorized to use other, unsanctioned Remote Access tools, including popular commodity Remote Access tools.

3.6.1 The sanctioned University VPN uses SSO services and requires Multi-Factor Authentication for all users, including third parties.

3.6.2 Exceptions may be granted on a case-by-case basis after review by the Information Security Office and implementation of appropriate compensating controls to protect the University internal network and Controlled Data.

3.7 **Wireless (Wi-Fi) Networking:** The University provides extensive wireless networking services within its buildings and premises. These services are designed to meet the needs of nearly all use cases for employees, students, and other users. The University does not govern the radio frequencies used by wireless networking devices and therefore cannot expressly forbid the use of non-University wireless network access points, routers, and/or other devices that offer wireless services in public RF spectrum. However, employees and students are not permitted to connect these non-University wireless access devices to the wired University network. Wired network ports connected to any unauthorized non-University wireless devices will be turned off upon discovery. To ensure the best experience for all users, the University strongly encourages employees and students to use University provided wireless networking services and not to bring or operate additional wireless devices within the University campus.

3.7.1 Exceptions may be granted on a case-by-case basis after review and approval by Network Services and the Information Security Office, and implementation of appropriate compensating controls to protect the University internal network and Controlled Data.

Policy Owner: Vice President of Administrative Affairs
Policy Steward: Chief Information Officer

History:
Approved 4/28/17
Revised 11/10/23