Utah Tech University Policy

463: Information Technology Security

I. Purpose

1.1 Utah Tech University ("the University") operates an extensive Information Technology infrastructure for the use and benefit of students, faculty, and staff and the fulfilment of its mission as a University of higher education. The University also collects, creates, and utilizes information about its students and employees and internal operation. This policy defines the responsibilities and actions needed to maintain secure University information technology infrastructure, protect information held in trust by the University, and ensure that risk-based decisions regarding the use of information and technology infrastructure are made at the appropriate levels of University administration.

II. Scope

2.1 This policy will apply to all Utah Tech University constituents who use, maintain, store, or otherwise deal with information within the University information technology environment. This policy also applies to all University constituents who use or access University-owned, personal, or third-party information technology resources to conduct University business or functions.

III. Definitions

3.1 ***Branded Payment Cards:*** Credit and debit cards issued by major international payment brands.

3.2 ***Center for Internet Security (CIS) Critical Security Controls:*** An industry standard set of prioritized and prescriptive cybersecurity best practices. The CIS standards provide specific guidance for organizations to create

and maintain successful information security programs and meet the requirements and objectives of multiple legal, regulatory, and policy frameworks.

3.3 ***Data***

3.3.1 ***Controlled Data:*** Information or data for which there is a requirement or expectation that the collection or creation of, access to, use, disclosure, and/or destruction of said information be protected and controlled at the University. Controlled Data is defined in two categories, restricted and internal:

3.3.1.1 ***Restricted Data:*** Information or data collected from or maintained about students, employees, alumni, or other University constituents that is confidential or private in nature. Additionally, other non-personal information may be considered restricted as defined by Federal/State law or contract. Access, use, protection and disclosure of Restricted Data are typically controlled by one or more of the following: Federal and State law or regulation, contract, and/or other applicable policies developed by the Utah Board of Higher Education or Utah Tech University.

3.3.1.1.1 Examples of Restricted Data include, but are not limited to, any non-directory Family Educational Rights and Privacy Act (FERPA) information, Social Security numbers, medical records, individual passwords, personal financial data including bank account and credit card numbers, certain research data, or government-classified data. If stored with any of the preceding information elements in a record or if disclosed in an extraordinary or uncontrolled manner, information normally classified as directory information under FERPA, such as name, address, date of birth, major, class, etc., may also be considered restricted.

3.3.1.2 ***Internal Data:*** Information or data collected, processed, stored, or otherwise used by the University that are sensitive, proprietary, or otherwise expected to be kept confidential but are not otherwise classified or controlled as Restricted Data. Access, use, protection, and disclosure of Internal Data may be controlled by one or more of the following: Federal and State law or regulation, contract, and/or other applicable

policies developed by the Utah Board of Higher Education or Utah Tech University.

3.3.1.2.1 Examples of Internal Data may include, but are not limited to, University financial records, research data, IT and/or facilities systems configuration, surveillance video, personnel records, or contracts and purchasing records.

3.3.2 ***Critical Data:*** Information that is required for continuing operation of the University and its critical functions. Failures or loss of critical IT resources could result in loss of critical University functions, create public safety issues, cause significant fiscal losses or incur legal liability.

3.3.3 ***Institutional Data:*** All data elements relevant to operations, unit-level planning and management of any unit, data that are reported or used in official University reports, and data that reside in or are generated as a result of utilizing enterprise transactional systems.

3.3.4 ***Uncontrolled Data:*** Information or data collected, processed, stored or otherwise used by the University for which there is no expectation of confidentiality nor any special protections or controls needed.

3.4 ***Data Governance:*** University governance processes defined by Policy 120 "Institutional Data Governance" and Policy 461 "Stewardship of IT Resources" shall determine how data and IT resources are classified and recognized within the University.

3.5 ***Data Trustee:*** A cabinet-level position responsible for Institutional Data and IT Resources at the policy level.

3.6 ***Data Steward:*** A position that is operationally or administratively responsible for Institutional Data and/or IT Resources.

3.7 ***Incident Response Team:*** The Incident Response Team is a group convened when the Information Security Office determines the scope, size, or nature of an Information Security incident warrants additional response resources. The Incident Response Team is coordinated by ISO and may be comprised of Data Stewards, University and/or third-party subject-matter experts, and other stakeholders as deemed appropriate for the incident.

3.8 ***Information Security Office:*** The Information Security Office (ISO) is

responsible for developing and coordinating University Information Security strategies.

3.9 ***Information Technology Resource (IT Resource):*** IT systems, infrastructure, or media that provides essential services to core University functions or that display, process, transmit, store, or otherwise utilize data.

3.9.1 ***Official University IT Resource:*** IT resources sanctioned by University Data Governance processes and provided by University Information Technology Services, or IT Resources that are hosted or are on the "cloud" that have been sanctioned by the University Data Governance processes and for which the University has contracted with a third party to provide essential services to core University functions and/or that display, process, transmit, store, or otherwise utilize data that are classified as Institutional Data, Controlled Data, and/or Critical Data.

3.9.1.1 Examples include, but are not limited to, the University network, Banner system, Canvas learning management system, email system, identity management systems, storage, Utah Tech University website, any sanctioned third-party equivalents, and various other servers and infrastructure. A University-owned workstation may be considered an Official IT Resource when it is centrally managed and meets security standards established and published under the authority of this policy.

3.9.2 ***Personal IT Resource:*** Any IT resource not owned or otherwise provided by the University.

3.9.3 ***Portable Devices and Media:*** An IT resource used to display, process, transmit or store data that is easily portable.

3.9.3.1 Examples include, but are not limited to, laptop computers, smartphones, tablet computers, optical media, magnetic tapes, removable hard drives, flash memory devices (USB thumb drives, memory cards) and other portable devices with storage capabilities.

3.10 ***Unauthorized Access:*** Access to Controlled Data or to IT Resources by individuals or automated agents that are not authorized for access to perform job duties or University functions.

3.11 ***User:*** Any University employee or other affiliate who accesses and uses

University data and/or IT Resources.

IV. Policy

4.1 Roles and Responsibilities

4.1.1 Each Data Trustee, for information, data or resources within the Data Trustee's respective area of operation, shall be responsible to:

4.1.1.1 Determine the security classification (e.g., Controlled Restricted, Controlled Internal) of data, as defined by and outlined in this policy.

4.1.1.2 Understand the regulatory and legal requirements governing Controlled Data and direct appropriate compliance efforts.

4.1.1.3 Maintain an inventory of Restricted Data collected, stored, used, and/or transmitted.

4.1.1.4 Evaluate threats and risks to Controlled Data and act as the primary decision-maker for use of Controlled Data, as advised by the Information Security Office, Data Governance Committee, the University CIO, and other appropriate persons or entities.

4.1.1.5 Authorize access to and use of Controlled Data, or explicitly delegate these authorization responsibilities to an appropriate deputy.

4.1.1.6 Ensure that data classified as Institutional Data, Controlled Data, and/or Critical Data are stored and used only within Official University IT Resources.

4.1.1.7 Assist in enforcement of University information security practices.

4.1.1.8 Authorize and accept responsibility for any exceptions to University security practices as defined by this policy and addenda.

4.1.2 Each Data Steward, for data or IT Resources within the Data Steward's respective area of operation, shall be responsible to:

4.1.2.1 Understand the security classification (e.g. Controlled Restricted, Controlled Internal) of the data and follow University information security practices appropriate to that

classification.

4.1.2.2 Understand the regulatory and legal requirements governing Controlled Data and establish and follow appropriate compliance measures.

4.1.2.3 Ensure that decisions on access to and use of Controlled Data are made by the appropriate Data Trustee or delegated deputy.

4.1.2.4 Release Institutional Data and/or Controlled Data only through appropriate, established channels.

4.1.2.5 Assist Data Trustees in inventorying use of Restricted Data collected, stored, used, and/or transmitted on IT Resources. Ensure that data classified as Institutional Data, Controlled Data, and/or Critical Data are stored and used only within Official University IT Resources.

4.1.2.6 Assist in enforcement of University information security practices.

4.1.2.7 Report any unauthorized access or suspected security incident/breach to ISO in a timely manner.

4.1.3 The Information Security Office shall be responsible to:

4.1.3.1 Develop and maintain University information security policies and practices in coordination with Data Trustees and Data Stewards. Develop and prioritize these University security plans and practices as informed by the CIS standards, other applicable legal or regulatory frameworks, and the current risk/threat environment. Advise and assist Data Trustees and Stewards in establishing appropriate compliance measures for Controlled Data.

4.1.3.2 Educate and provide assistance to Data Trustees, Data Stewards and Users in complying with this policy and security practices.

4.1.3.3 Operate and/or coordinate appropriate security measures for protection of IT Resources.

4.1.3.4 Monitor network traffic and IT operations to identify, evaluate, and mitigate threats or vulnerabilities to University Controlled Data and/or IT Resources, and to assess

compliance with University security policies and practices.

4.1.3.5 Take appropriate and reasonable action to resolve security incidents. Direct incident response activities and incident resolution, including convening the University Information Security Incident Response Team, if necessary.

4.1.3.6 Conduct periodic security assessments to identify evolving threats and vulnerabilities to the security of University data and IT Resources, and to evaluate compliance with information security policies and practices.

4.1.3.7 Enforce University security policies and practices in coordination with Data Trustees and Data Stewards.

4.1.4 Users shall be responsible to:

4.1.4.1 Understand and follow University policies and practices governing the use of IT Resources and Controlled Data.

4.1.4.2 Report any unauthorized access or suspected security incident/breach to ISO in a timely manner.

4.1.5 The Incident Response Team, when convened, shall be responsible to:

4.1.5.1 Under the direction of the ISO, contain and resolve security incidents as directed by Addendum 463b, Information Security Incident Response Procedures.

4.2 Protection of Controlled Data

4.2.1 Controlled Data, including Restricted Data and Internal Data, must be protected in all phases of its lifecycle, including creation/collection, use, storage, transmission, and disposal, such that the Controlled Data remains confidential.

4.2.1.1 Controlled Data must not be disclosed or released except through channels and procedures established by the appropriate Data Trustee(s) and/or University Data Governance processes.

4.2.2 Controlled Data must be stored, transmitted, and/or used only within Official University IT Resources. Controlled Data must not be stored, transmitted or used on unmanaged workstations, an unmanaged Portable Computing Device and Media, a Personal IT

Resource, or third-party "cloud" or hosted services that are not sanctioned or approved as an Official University IT resource.

4.2.3 A third-party "cloud" or hosted service is considered an Official University IT Resource suitable for collection, use, or storage of Controlled Data only when sanctioned through University Data Governance processes and when an appropriate contract or Memorandum of Understanding is in place that protects the University's interests and outlines security measures to be taken on the part of the third-party provider. Whenever possible, administrative access to and control of data held in trust by the third-party provider should be available to University Information Technology staff. Integration with the University Digital ID identity and authentication systems must also be used whenever possible.

4.2.4 Exceptions to Protections established by this policy may be approved in the following circumstances:

4.2.4.1 Faculty members without access to a managed University workstation may enter, view, and/or manipulate academic grades, assignment scores, and/or other academic records related to student course performance using an unmanaged workstation or device. The unmanaged device may be used to enter, view, and/or manipulate these records stored within an Official University IT Resource (i.e., Canvas, Banner), so long as the academic grades or records are not stored on the unofficial, unmanaged device; or

4.2.4.2 All of the following:

4.2.4.2.1 There is a business need for Controlled Data to be stored, or used outside of Official University IT Resources that cannot otherwise be met;

4.2.4.2.2 The Data Trustee(s) over the Controlled Data in question must be made aware of the request for exception, be apprised of any risks in granting an exception, and approve of the departure from standard practice;

4.2.4.2.3 An inventory of the nature of, the location or disposition of, and the number of records of the Controlled Data must be maintained by the department or unit and provided to the Data Trustee and ISO; and,

4.2.4.2.4 Appropriate, documented, and auditable protections for the Controlled Data are in place.

4.2.5 Access to Controlled Data should only be granted to individuals and entities who need access to perform their designated job function, contracted services on behalf of the University, or to meet some other regulatory or legal requirement. Data Trustees and/or their designated deputies must authorize access to Controlled Data.

4.2.5.1 Effective 7/1/2024, Data Stewards and Users accessing Controlled Data must sign a University Confidential Data Agreement. Data Trustees, or a designated deputy to grant access, must ensure this Agreement is signed before granting access to Controlled Data.

4.2.5.2 Faculty accessing Controlled Data only for the purposes of managing their own courses (e.g., grading) are not required to sign a University Confidential Data Agreement. However, faculty are expected to keep confidentiality of these records as defined by this policy and FERPA regulations.

4.2.6 Controlled Data must be protected pursuant to the current security measures as outlined in Addendum 463a University Information Security Rules and Standards.

4.2.7 Industry regulation of Branded Payment Cards imposes additional security requirements for University departments or other units accepting Branded Payment Cards. These requirements are defined by the Payment Card Industry Data Security Standards (PCI-DSS). Before conducting commerce or otherwise collecting University funds using Branded Payment Cards, departments and units must be granted approval from University Business Services. Departments and units accepting Branded Payment Cards must adhere to practices developed to protect credit card holder information as required by the University Cash Handling policy, currently published PCI-DSS standards, and internal requirements and guidance maintained by the University Payment Card (PCI) Committee.

4.3 Reporting and handling of IT Security Incidents

4.3.1 All suspected or actual IT security incidents involving University or departmental data, or IT Resources must immediately be reported to the Information Security Office.

4.3.2 ISO is authorized to take or direct reasonable action as necessary to neutralize a security incident or prevent further damage, including but not limited to, disabling user accounts, blocking network traffic, and disabling services.

4.3.3 ISO will coordinate response, investigation and reporting of information security incidents as defined in procedure Information Security Incident Response. If necessary, ISO will convene the Incident Response Team to assist in handling the incident. ISO and/or the Incident Response Team work to contain or mitigate any unresolved threat stemming from the incident to IT Resources or data. ISO and/or the Incident Response Team reports findings and recommendations regarding the incident to University administration and appropriate Data Trustees.

4.3.4 If it is determined that University constituents must be notified of disclosure or loss of Controlled Data, efforts must be coordinated between responsible Data Trustees, ISO, University Office of General Counsel, University public relations, and other stakeholders as necessary to ensure that notification is performed by, or on behalf of, the responsible Data Trustee in a timely manner in accordance with Federal and State notification laws and regulations. Refer to Addendum 463b, Incident Response.

4.4 Physical Information Security – University departments and units are responsible for assuring that all Controlled Data, whether in digital or physical format, and IT Resources are physically protected at all times in accordance with their level of criticality and sensitivity. University departments and units must assure that the physical information security controls for work area are followed and that access restrictions, Controlled Data security practices and physical security practices for each area are adhered to.

4.5 Destruction or sanitization of electronic media – Departments and University units must destroy or otherwise sanitize Controlled Data stored on IT Resources when the data is no longer necessary to conduct the business of the University, meet regulatory requirements, or when hardware or media devices are retired or repurposed.

4.6 Additional procedure and practices – This policy authorizes Data Trustees, Data Stewards, ISO, and Information Technology Services to develop additional Information Security procedures and guidance in accordance with the requirements and intent of this policy. Data Trustees and Stewards may implement rules for the departments or units for which they

are responsible.

4.7 Revocation of Access

4.7.1 The University shall reserve the right to revoke access to the University network or any IT Resource for any internal or external user, device, network segment, or system which presents a direct and imminent threat to University IT Resources or information assets, violates this policy, violates attached procedures or established practices, or for any other reason in accordance with applicable University policies.

4.7.2 Restoration of Access – Access for a revoked user, device, network segment or system may be restored as soon as the direct and imminent security threat or policy violation has been remedied.

4.8 Policy Violations

4.8.1 Violation of this policy may result in action in accordance with University disciplinary policies.

4.8.2 University constituents may appeal revocation of access to IT Resources or disciplinary actions taken against them pursuant to University grievance policies.

V. References

5.1 Utah Board of Higher Education Policy R345, Information Technology Resource Security

5.2 University Policy 120: Institutional Data Governance

5.3 University Policy 121: Institutional Data

5.4 University Policy 201: Cash Handling and Income Recognition

5.5 University Policy 151: Grievance Procedure

5.6 University Policy 372: Corrective & Disciplinary Action

5.7 University Policy 461: Stewardship of IT Resources

5.8 University Policy 462: Use of University IT Resources

5.9 Utah Tech University Confidential Information Agreement

VI. Procedures—N/A

VII. Addendum

7.1 463a: University Information Security Rules and Standards

7.2 463b: Incident Response Procedure

7.3 463c: University Information Security Data Classification Visual Aids

---

Policy Owner: Vice President of Administrative Services
Policy Steward: Chief Information Officer; Information Security Officer

History:
Approved 4/28/2017
Editorial 07/01/22
Revised 11/10/23