



# UTAH VALLEY UNIVERSITY

## Policies and Procedures

Page 1 of 42

<b>Proposed Policy Number and Title:</b> <b>447 Information Security</b>		
<b>Current Policy Number and Title:</b> 447 Information Security		
<b>Approval Process*</b>		
<input checked="" type="checkbox"/> Regular	<input type="checkbox"/> Temporary	<input type="checkbox"/> Compliance Change
<input type="checkbox"/> New <input checked="" type="checkbox"/> Revision <input type="checkbox"/> Revision—Limited Scope <input type="checkbox"/> Deletion	<input type="checkbox"/> New <input type="checkbox"/> Revision <input type="checkbox"/> Revision—Limited Scope	<input type="checkbox"/> New <input type="checkbox"/> Revision—Limited Scope <input type="checkbox"/> Deletion
*See UVU Policy 101 <i>Policy Governing Policies</i> for process details.		

<b>Draft Number and Date:</b>	<u>Stage 3 Regular, May 1, 2025</u>
<b>President's Council Sponsor:</b>	<u>Christina Baum</u>
<b>Policy Steward:</b>	<u>Brett McKeachnie</u>

POLICY APPROVAL PROCESS DATES		
REGULAR	TEMPORARY	COMPLIANCE
<b>Drafting and Revision</b> Entrance Date: <u>5/23/2024</u>	<b>Drafting and Revision</b> Entrance Date: <u>N/A</u>	<b>President's Council Approval</b> Approval Date: <u>N/A</u>
<b>University Entities Review</b> Entrance Date: <u>2/13/2025</u> Close Feedback: <u>4/10/2025</u>	<b>Board of Trustees Review</b> Entrance Date: <u>N/A</u> Approval Date: <u>N/A</u>	<b>Board of Trustees Ratification</b> Ratification Date: <u>N/A</u>
<b>Board of Trustees Review</b> Entrance Date: <u>5/8/2025</u> Approval Date: _____		



# UTAH VALLEY UNIVERSITY

## Policies and Procedures

Page 2 of 42

<b>POLICY TITLE</b>	Information Security	<b>Policy Number</b>	447
<b>Section</b>	Facilities, Operations, and Information Technology	<b>Approval Date</b>	
<b>Subsection</b>	Information Technology	<b>Effective Date</b>	
<b>Responsible Office</b>	Office of the Vice President of Digital Transformation	<b>Last Review</b>	

### 1.0 PURPOSE

1.1 The purpose of this policy is to establish the Utah Valley University Information Security Program in compliance with all applicable legal obligations. This program will ensure the protection of university technology assets and information systems from unauthorized access or damage; and maintain the confidentiality, integrity, and availability of technology assets and information systems supporting the mission and functions of the University.

### 2.0 REFERENCES

- 2.1 *Family Educational Rights and Privacy Act (FERPA)*, 20 U.S.C. § 1232g (1974)
- 2.2 *Federal Information Security Management (FISMA)*, 44 U.S.C. § 3541 (2002)
- 2.3 *American Recovery and Reinvestment Act of 2009*, Pub. L. No. 111-5, 123 stat 115 (2009)
- 2.4 *Offenses Against the Administration of Government*, Utah Code Ann. § 76-8-703 and -705 (2013)
- 2.5 *Interception of Communications Act*, Utah Code Ann. § 77-23a-1 (1980)
- 2.6 Utah Board of Higher Education Policy R345 *Information Technology Resource Security*
- 2.7 UVU Policy 133 *Compliance with Government Records Access and Management Act*
- 2.8 UVU Policy 136 *Intellectual Property*
- 2.9 UVU Policy 241 *University Procurement*
- 2.10 UVU Policy 309 *Executive Employees: Recruitment, Compensation, Termination*
- 2.11 UVU Policy 371 *Corrective Actions and Termination for Staff Employees*
- 2.12 UVU Policy 445 *Institutional Data Governance and Management*



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 3 of 42

- 19 **2.13** UVU Policy 446 *Privacy and Disclosure*
- 20 **2.14** UVU Policy 448 *Authorization and Management of Web, Internet, and Domains*
- 21 **2.15** UVU Policy 451 *Retention of Electronic Files*
- 22 **2.16** UVU Policy 457 *PCI DSS Compliance*
- 23 **2.17** UVU Policy 541 *Student Code of Conduct*
- 24 **2.18** UVU Policy 635 *Faculty Rights and Professional Responsibilities*

### 3.0 DEFINITIONS

- 25 **3.1 Account:** A login ID which, in combination with a password, PIN, or other authentication  
26 token, is used to access a university information system or technology asset.
- 27 **3.2 Application:** An individual or standalone piece of software that is used to provide a specific  
28 service to a community of users or is used as an interface to an information system.
- 29 **3.3 Audit log:** A chronological sequence of audit records, each of which contains evidence  
30 directly pertaining to and resulting from the execution of a business process or system function.
- 31 **3.4 Change:** For purposes of this policy, an event or action that modifies the configuration of  
32 any component, application, information system, or service.
- 33 **3.5 Confidential information:** Any information that is not generally available to the public and  
34 that the University has identified as confidential, that should reasonably be understood to be  
35 confidential, or that the University is obligated to keep confidential under applicable laws,  
36 regulations, contractual obligations, university policies, or the policies of relevant government  
37 agencies, including but not limited to PII, student records, financial information, research data,  
38 and sensitive information.
- 39 **3.6 Control:** A means of managing risk, including policies, rules, procedures, processes,  
40 practices, or organizational structures, which can be of administrative, technical, physical,  
41 management, or legal nature.
- 42 **3.7 Crash:** A disruption of the supervisory or accounting functions of university technology  
43 assets or doing anything that is likely to have that effect.
- 44 **3.8 Data Governance Council:** An executive committee with specific responsibilities within a  
45 data domain or subdomain: data owners, data trustees, data stewards, data custodians, and data  
46 technicians. (See Policy 445 *Institutional Data Governance and Management*.)



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 4 of 42

**3.9 Device owner:** For the purposes of this policy, any user, supervisor, IT technician, system administrator, or other person who has administrative or operational control and is responsible for the security, maintenance, operation, or purchase of a device.

**3.10 Disruptive activities:** Acts prohibited by Utah law that interfere with university or student activities. (See Utah Code Ann. § 76-8-703 to 705.)

**3.11 Encryption:** The process by which information is altered using a code or mathematical algorithm to be unintelligible to unauthorized readers.

**3.12 Firewall:** A network security device or program that monitors and controls network traffic between networks or hosts with different security levels.

**3.13 Incident:** For the purposes of this policy, an incident is a confirmed or suspected security breach (see section 3.25) or events or weaknesses that jeopardize the confidentiality, integrity, and availability of the University's technology assets.

**3.14 Incident Response Team:** Directed by the Chief Information Security Officer (CISO) and made up of campus personnel, the Incident Response Team is responsible for immediate response to any breach of security. One or more members of the Incident Response Team must be technically qualified to respond to information-related incidents. The Incident Response Team is also responsible for determining and disseminating remedies and preventive measures that develop as a result of responding to and resolving security breaches.

**3.15 Information asset:** Data or knowledge stored in any electronic manner and valued for enabling the University to perform its business functions.

**3.16 Information system:** An application or group of servers or services used for the electronic storage, processing, or transmitting of any university data or information assets.

**3.17 Information system media:** Physical media on which an information system's technology assets are stored for backup and recovery purposes (e.g., backup tapes, backup disks, NAS/SAN drives, magnetic media, cloud storage, etc.).

**3.18 Intellectual property:** Any intangible asset that consists of human knowledge and ideas (e.g., patents, copyrights, trademarks, software, etc.).

**3.19 IT technicians:** Individuals who develop, administer, manage, and monitor the information systems and technology assets that support the University's IT infrastructure. These individuals are responsible for the security of the technology assets and information systems they manage. IT technicians ensure that security-related activities are well documented and completed in a consistent and auditable manner.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 5 of 42

**3.20 Patch:** A fix to an application, failure, bug, or vulnerability. A patch may also be referred to as a service pack.

**3.21 Personally identifiable information (PII):** Unique identifiers, including a person's Social Security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, and personal email addresses.

**3.22 Private Sensitive Information (PSI):** A subset of PII that includes information such as social security numbers, credit card information, health, and medical records or financial records, that give specific information about an individual that is considered private or sensitive and can lead to adverse consequences if disclosed, such as through identity theft, financial loss, or invasion of privacy. Access to such data is governed by state and federal laws, both in terms of protection of the data, and requirements for disclosing the data to the individual to whom it pertains. It does not include "public information" as defined by GRAMA or directory information as defined by FERPA.

**3.23 Risk:** The likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact.

**3.24 Routine maintenance of the system:** Includes but is not limited to security checks, deletion of temporary files, verification of email delivery, and confirmation of available disk space.

**3.25 Security breach:** Includes but is not limited to unauthorized use of an account, unauthorized access or unauthorized changes to system resources, use of bad passwords, or attempted use or acquisition of others' passwords or other authentication methods.

**3.26 Security check:** Verification that privacy is ensured, and access is granted as needed and appropriate.

**3.27 Server:** Hardware, software, and workstations used to provide information and services to multiple users.

**3.28 System files:** Any files that control or otherwise affect the startup or operation of a computer system.

**3.29 Technology asset:** Any data or information system which is a part of university business processes including those used for electronic communication, including but not limited to internet, email, and social media. Also includes any device that is used to conduct university business regardless of ownership; connected to the University's network; used to create, access, maintain, or transmit technology assets; or used for the processing, transmitting, or electronic storage of any data or information. This includes but is not limited to servers, workstations,



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 6 of 42

mobile devices, medical devices, networking devices, and web cameras or other monitoring devices.

**3.30 Unauthorized access:** Obtaining access into any technology asset, information system, network, storage medium, system, program, file, data, user area, controlled physical area, or other private repository without the permission of the steward or owner.

**3.31 User:** Any person who accesses any university technology asset, including students, staff, faculty, permanent and temporary employees, contractors, vendors, research collaborators, and third-party agents.

**3.32 Vulnerability:** A weakness that could be used to endanger or cause harm to an asset.

**3.33 Workstation:** A technology asset that performs as a general-purpose computer equipped with a microprocessor and designed to run applications for an individual user (e.g., laptop, desktop computer, PC, Mac, etc.).

## 4.0 POLICY

### 4.1 Scope of this Policy

**4.1.1** Compliance with this policy and all its related procedures is required for all university administrative units, including colleges, divisions, departments, and centers, and all members of the university community, including students, staff, faculty, other permanent or temporary employees, contractors, research collaborators, vendors, and third-party agents. This policy applies to anyone in the university community owning or overseeing the use of any type of technology asset, including but not limited to

**4.1.1.1** supervisors of university entities or units, even in cases where vendor-owned or vendor-managed equipment is housed in departments;

**4.1.1.2** faculty, staff, students, and other individuals who have technology assets connected to the UVU network, even if those assets were acquired personally, i.e., not with university or grant funds; and

**4.1.1.3** Digital Transformation (Dx) for the enterprise IT devices under ongoing support contracts.

**4.1.2** If no one claims responsibility for a device, the supervisors of university entities or units for the department in which the device resides shall be presumed to be responsible by default.

**4.1.3** This policy applies to individuals responsible (as defined above) for single-user devices and to those responsible for multi-user devices.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 7 of 42

4.1.4 During routine audits, Internal Audit may verify user compliance with this policy and security requirements.

#### 4.2 User Responsibilities

4.2.1 Use of technology assets must be legal, ethical, and consistent with the University's mission.

4.2.2 Instructional, administrative, and research uses of technology assets take priority over all other uses.

4.2.3 Individual users shall

4.2.3.1 maintain the security and confidentiality of confidential information;

4.2.3.2 exercise caution in the storage and disposal of files and data containing confidential information assets;

4.2.3.3 maintain safe passwords and other authentication methods, and not share or disclose them;

4.2.3.4 perform routine maintenance of the systems for which they are responsible, including backup of all private, important, or irreplaceable files, and regularly performing file maintenance (including scanning for viruses and sensitive data and deleting unnecessary files);

4.2.3.4.2.3.5 configure their computers and mobile devices to automatically lock the screen after a period of inactivity, and must manually lock their screens when leaving their devices unattended to prevent unauthorized access.

4.2.3.5.4.2.3.6 ascertain and understand the laws, policies, rules, procedures, contracts, and licenses applicable to their particular uses;

4.2.3.6.4.2.3.7 comply with all federal, state, and other applicable laws, all generally applicable university policies, guidelines, procedures, and best practices, and all applicable contracts and licenses;

4.2.3.7.4.2.3.8 use only those information systems and technology assets that they are authorized to use and use them only in the manner and to the extent authorized;

4.2.3.8.4.2.3.9 refrain from unauthorized attempts to circumvent the security mechanisms of any university technology asset;

4.2.3.9.4.2.3.10 refrain from attempts to degrade system performance or capabilities or damage technology assets, information systems, software, or intellectual property of others;



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 8 of 42

[4.2.3.104.2.3.11](#) use multi-factor authentication required for all administrative and functional access to technology assets that store, process, or transmit personally identifiable information; and

[4.2.3.114.2.3.12](#) immediately report any suspected or actual security breach to the University's Cybersecurity and IT Risk Management Office (CITRM), the appropriate data steward, and data custodian.

**4.2.4** Employees are required to follow Dx standards and controls for safeguarding electronically stored PSI. The University and its employees should not use an individual's Social Security Number (SSN) or Driver's License Number (DLN) as a personal identifier except as required by law. Restricted information, including SSNs and DLNs, may be stored electronically only in compliance with current Dx standards. If restricted information must be stored on paper, the files must be stored securely with access provided only to authorized persons.

**4.2.5** All data users who have access to legally restricted or limited-access data shall formally acknowledge (by signed statement or some other means) their understanding of the level of access provided and their responsibility to maintain the confidentiality of data they access. Each data user shall be responsible for the consequences of any misuse, including intentional misrepresentation of institutional data. (See Policy 445 *Institutional Data Governance and Management*.)

### **4.3 User Prohibitions**

**4.3.1** Users shall not

**4.3.1.1** share individual credentials or security information;

**4.3.1.2** copy or change system files or applications without authorization from an authorized system administrator;

**4.3.1.3** consume inordinate amounts of system resources (e.g., disk space, CPU time, email system, printing facilities, and telephone lines), as determined by affected system administrators;

**4.3.1.4** crash machines or systems recklessly or deliberately;

**4.3.1.5** lock a public shared technology asset without authorization from a supervisor or asset manager;

**4.3.1.6** use university technology assets for disruptive or illegal activities;

**4.3.1.7** violate licensing agreements, patent, copyright, or trademark laws or UVU Purchasing regulations as governed by UVU Policy 241 *University Procurement*;





## UTAH VALLEY UNIVERSITY

### Policies and Procedures

**4.3.1.8** reserve shared resources. A public shared computing facility device left unattended for more than ten minutes is available for use, and any process running at the time of abandonment shall be terminated. Running unattended programs or placing signs on devices to “reserve” them during a user’s absence is inappropriate without authorization from a system administrator or lab assistant; or

**4.3.1.9** use weak passwords. Users are required to create strong passwords to protect against security breaches. A strong password should be long, memorable to the user, and difficult for others to guess. We recommend creating passwords using multiple unrelated words to form a passphrase that is easy for you to remember but hard for others to crack. For example, combining random and unrelated words like “BananaLampTreeEagle” is a strong option. Do not use the following in your passwords:

- **Personal Information:** Avoid using information related to yourself, such as your phone number, birth date, license plate number, spouse’s name, or other identifiable details.
- **Common Phrases:** Do not use words like team mascots, seasons, or phrases from books, poems, songs, movies, or famous speeches.

**4.3.2** Unless specifically approved by the Data Governance Council and registered with University's Information Security Office (ISO) according to the procedures ([see 5.3.1](#)) in this policy, anyone given access to university data shall not electronically transmit or knowingly retain any PSI on information systems or technology assets.

## **4.4 System Administrator Rights and Responsibilities**

**4.4.1** System administrators must perform routine system maintenance and maintain a backup of information. System administrators are not responsible for data lost due to system errors.

**4.4.2** Dx, including system administrators, shall work in partnership with data owners and data stewards in fulfilling the responsibilities outlined in this policy.

## **4.5 Intellectual Property Use**

**4.5.1** All users of intellectual property shall comply with UVU Policy 136 *Intellectual Property*, including refraining from

**4.5.1.1** installing or distributing "pirated" or other applications that are not appropriately licensed for use by the University; and

**4.5.1.2** violating the rights of any person or company protected by trade secret, patent, or any other intellectual property laws or similar laws or regulations.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 10 of 42

#### 4.6 Data Classification and Encryption

4.6.1 The University shall take measures to protect university technology assets that are created, maintained, processed, or transmitted using information systems and information assets. These measures shall be implemented commensurate with the assessed level of risk and reviewed at regular intervals.

4.6.2 IT technicians are primarily responsible for establishing, documenting, implementing, and managing data handling and management procedures for the information systems and information assets they support.

4.6.3 All information assets shall be classified in accordance with the *Data Classification and Encryption Guideline*, which can be found on the Digital Transformation policies website.

4.6.4 All information assets shall have appropriate data handling procedures in accordance with the data classification.

4.6.5 All information assets shall have encryption requirements in accordance with the *Data Classification and Encryption Guideline*, which can be found on the Dx policies website.

#### 4.7 Information Security Risk and Threat Management

4.7.1 The University's Information Security Risk Management Program shall support the University's business missions while also mitigating financial, operational, reputational, and regulatory compliance risk. Appropriate risk management enables the University to accomplish its mission by

4.7.1.1 securing information systems that create, maintain, process, or transmit the University's information assets;

4.7.1.2 enabling appropriate university personnel to make well-informed decisions regarding risk and risk management;

4.7.1.3 collaborating with other university risk management activities to ensure the University's information security program priorities are aligned appropriately with the University's risk tolerance;

4.7.1.4 providing a systematic methodology to assess and manage information security risk for the University; and

4.7.1.5 reviewing contracts and terms of service to ensure that third parties entrusted with PII will implement reasonable protections for that information in all stages of its lifecycle including creation, storage, processing, recovery, transmittal, and destruction.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 11 of 42

**4.7.2** Information systems and technology assets shall be protected commensurate with the assessed level of risk, and security baseline settings shall be utilized to ensure these systems and resources are guarded against malware and available for use. All IT technicians, Dx personnel, and users managing university information systems and technology assets shall

**4.7.2.1** protect any information systems and technology assets under their management from compromise;

**4.7.2.2** ensure the products and services provided continue to be delivered at acceptable levels during a disruptive incident. Incidents may be caused by problems with technology assets, the building, or external environment (such as weather);

**4.7.2.3** configure information systems and technology assets to reduce vulnerabilities to an acceptable risk level;

**4.7.2.4** install anti-virus or other anti-malware tools, install relevant security patches, and implement security best practices for technology assets;

**4.7.2.5** periodically verify audit and activity logs, examine performance data, and check for any evidence of unauthorized access, viruses, or other malicious code; and

**4.7.2.6** cooperate with the Information Security Office by providing support for and review of administrative activities as well as performing more sophisticated procedures such as penetration testing (also called pen testing or ethical hacking) to test a computer system, network, or web application to find security vulnerabilities that an attacker could exploit along with real-time intrusion detection.

## **4.8 Access Management**

**4.8.1** Only authorized users shall have physical, electronic, or other access to information systems and technology assets. Access shall be limited to users with a business need to know and limited only to the requirements of their job function. It is the shared responsibility of IT technicians, data stewards, and users to prevent unauthorized access to these assets. Access controls shall include prevention and detection of unauthorized use, and effective procedures for granting authorization, tools, and practices to authenticate authorized users.

**4.8.2** The appropriate university system administration group shall

**4.8.2.1** issue university accounts after the request is authorized appropriately and documented adequately;

**4.8.2.2** authenticate university accounts at a minimum via unique login and complex passwords;



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 12 of 42

**4.8.2.3** deactivate, disable, or delete university accounts—except where maintaining such accounts is a business necessity—as soon as reasonably possible after receiving authorized notification of termination of contract, employment, or relationship with the University; and

**4.8.2.4** conduct periodic reviews of authorized access commensurate with the assessed level of risk.

#### **4.9 Change Management**

**4.9.1** Prior to implementation, Dx shall authorize, test, document, and approve any changes to university production information systems and technology assets that store, process, transmit, or maintain confidential data. Dx will notify the affected entities.

#### **4.10 Physical and Facility Security**

**4.10.1** University technology assets and information systems shall be physically protected commensurate with the assessed level of risk. IT technicians and personnel shall ensure that controls are planned and implemented for safeguarding physical components against compromise and environmental hazards. Locks, cameras, alarms, redundant power systems, fire detection and suppression systems, and other safeguards as appropriate shall be installed in data centers and technology closets to ensure protection from natural and facility threats and to discourage and respond to unauthorized access to electronic or physical components contained in these areas.

**4.10.2** The University shall maintain an inventory of all internal or third-party technology assets that store, process, or transmit personally identifiable information.

#### **4.11 Remote Access**

**4.11.1** Users with remote access privileges to any of the University's networks inside a firewall must connect through an approved connection method such as a secure VPN.

**4.11.2** Users with remote access privileges to the University's technology assets must ensure that all devices being used are given the same security considerations as outlined in the IT security annual training. Specific security questions should be directed to the Cybersecurity and IT Risk Management Office (CITRM).

#### **4.12 Network Security**

**4.12.1** Access to both internal and external networked services shall be controlled and protected commensurate with the assessed level of risk. User, information system, and technology asset access to networks and network services shall not compromise the security of the network services. Dx ensures



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 13 of 42

4.12.1.1 appropriate controls are in place between the University's network, networks owned by other organizations, and public networks; and

4.12.1.2 appropriate authentication mechanisms are applied for users, information systems, and technology assets.

#### 4.13 Log Management and Monitoring

4.13.1 The appropriate Dx personnel, in coordination with the CISO, shall configure university information systems and technology assets to record and monitor information security incidents, events and weaknesses. They shall regularly review and analyze audit logs for indications of inappropriate or unusual activity.

#### 4.14 Information System Media Handling

4.14.1 The University shall inventory, control, and physically protect information system media commensurate with the assessed level of risk and the *Data Classification and Encryption Guideline* to prevent interruption to business activities or unauthorized disclosure, modification, removal, or destruction of technology assets. The University shall establish appropriate operating procedures to protect information system media, input/output data, and system documentation from unauthorized disclosure, modification, removal, and destruction.

4.14.2 The appropriate university system administration or security group shall restrict access to information system media to authorized individuals.

4.14.3 All institutionally owned computing devices, including removable storage devices, shall have industry standard encryption that renders the storage media of those devices reasonably unrecoverable by a third party; when this is not feasible, the University shall implement other reasonable controls.

4.14.4 The University shall physically control and securely store information system media on-site within controlled areas where appropriate and ensure any authorized off-site storage is, at minimum, secured at the same level as the on-site area.

4.14.5 The University shall protect and control information system media during transport outside of controlled areas and shall restrict the activities associated with transport of this media to authorized personnel.

4.14.6 Appropriate university personnel shall sanitize or destroy information system media containing confidential data prior to disposal or release for reuse in accordance with National Institute of Standards and Technology guidance.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 14 of 42

#### 4.15 Future Technology Needs Assessment

4.15.1 Dx shall ensure the availability, performance, and capacity requirements for current and future needs are met with cost-effective service provision. This includes assessment of current capabilities, future needs based on organization requirements, and implementation of actions to meet the new requirements. Through effective capacity planning, Dx will ensure service availability, efficient management of resources, and optimization of system performance.

#### 4.16 Information Security Awareness and Training

4.16.1 All university employees and other affiliates are required to complete appropriate security training relevant to their roles and responsibilities before gaining access to systems, records, and information resources and shall renew that training annually. If university employees and other affiliates do not fulfill these training requirements, their access may be subject to revocation.

4.16.2 The relevant university information systems and security teams shall monitor developments in recognized security practices, methodologies, and technologies, as well as maintain awareness of emerging threats, vulnerabilities, and security incidents. ~~The appropriate university information systems and security groups shall stay up to date with the latest recommended security practices, techniques, and technologies, and the latest security-related information including threats, vulnerabilities, and incidents.~~

#### 4.17 Internal Audit Assessment

~~4.17.1 Internal Audit may audit information systems and technology assets to assess compliance with this policy.~~

#### ~~4.18.14.17~~ 4.17 Violations

~~4.18.14.17.1~~ 4.17.1 Incidents of actual or suspected non-compliance with this policy or associated regulations must be reported to the Cybersecurity and IT Risk Management Office (CITRM), whose administrators will work with the appropriate authorities to resolve the issue.

~~4.18.24.17.2~~ 4.17.2 The University reserves the right to revoke access to any information system or technology asset for any user who violates this policy or associated regulations or for any other business reasons in accordance with applicable policies. Violations of this policy or associated regulations may result in other disciplinary action in accordance with pertinent university policies.

#### ~~4.19.14.18~~ 4.18 Security Standards

~~4.19.14.18.1~~ 4.18.1 Those responsible for devices connected to the UVU network must ensure that key security vulnerabilities are eliminated from these devices.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 15 of 42

**4.19.24.18.2** Dx shall maintain and communicate to device owners a current list of key vulnerabilities and steps required to mitigate the vulnerabilities. Device owners are responsible for addressing those vulnerabilities promptly with Dx assistance as needed.

#### **4.20.19 Enforcement**

**4.20.14.19.1** In cases where information systems and technology assets are threatened by improperly maintained computing devices, Dx may eliminate the threat, working with the relevant device owner where possible. This may include denial of access.

#### **4.21.20 Exceptions to Policy**

**4.21.14.20.1** Exceptions to this policy must be justified, approved, and reviewed annually as outlined in the procedures. Requests for exceptions to this policy shall be made in writing to the Chief Information Officer. Exception may be granted if the benefits to the University far outweigh the risks of the vulnerable device, as judged by the Chief Information Officer.

#### **4.22.21 Review and Maintenance of Policy**

**4.22.14.21.1** Dx Executive Leadership, including the Chief Information Officer, shall review this policy at least annually and evaluate changes in law and technology that may impact the University. The committee shall invite representatives of UVUSA, PACE, General Counsel, and Faculty Senate to participate.

## **5.0 PROCEDURES**

### **5.1 Physical Security of Enterprise Hardware**

**5.1.1** Any department that assumes responsibility for administrative data must ensure that the computing systems housing the data are physically secure. Areas to address include the following:

**5.1.1.1** The equipment shall be protected from excessive heat, cold, humidity, and dryness. Alarms shall exist to warn of thresholds being exceeded;

**5.1.1.2** The equipment shall be protected against electrical interruptions, voltage spikes, and surges; and

**5.1.1.3** The equipment shall be protected with smoke detectors, fire extinguishers, and air-tight computer rooms for containment of fire suppression gas, air filters, and water sensors. Alarms tied to the University and city police departments shall be installed;

**5.1.1.4** The equipment shall be properly locked up with no vulnerabilities from drop ceilings, raised floors, or ventilation ducts. A log of accesses by personnel shall be kept; and



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 16 of 42

5.1.1.5 All backups shall, whether stored onsite or offsite, be securely maintained and managed in a manner appropriate for the storage of university data;

5.1.1.6 The history of theft and vandalism in the buildings of the immediate vicinity shall be considered, and appropriate measures shall be taken to counteract the risks; and

5.1.1.7 A disaster recovery plan shall exist, and drills shall be conducted on a regular basis. Offsite documentation shall exist, and key personnel shall be cross trained to handle an emergency.

5.1.2 Device owners shall install and run campus approved anti-virus software on these devices and apply updates from the software vendor as they become available.

5.1.3 Devices owners shall apply security-related updates to the operating system running on their devices as these updates become available from operating system vendors.

5.1.4 Device owners shall switch off unneeded services or use a firewall to eliminate the risk of these being exploited.

## 5.2 Incident Management

5.2.1 All suspected or actual security breaches of university or departmental systems must be reported immediately to the University's Chief Information Security Officer (CISO). (Reports may be emailed to SECURITY@UVU.EDU.) The incident must also be reported to the appropriate data steward and data custodian.

5.2.2 If the compromised system contains PII or PSI as outlined in UVU Policy 445 *Institutional Data Management and Access*, Dx personnel or the appropriate data owner must report the incident to the CISO. Additional technical, forensic, and other support may be sought from outside the campus community.

5.2.3 If PII, PSI, secured data, or any other information that must be safeguarded against unauthorized access has been accessed or compromised by unauthorized persons or organizations, IT personnel or the appropriate data owner must report the incident immediately to the CISO (SECURITY@UVU.EDU) and cooperate with their dean, department head, or supervisor; the Incident Response Team; their respective vice president; and the Office of General Counsel to assess the level of threat or liability posed to the University and to those whose PSI was accessed. In accordance with applicable laws, the University shall notify the individuals whose PSI was accessed or compromised, providing them with instructions regarding measures to be taken to protect themselves from identity theft.





## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 17 of 42

#### 5.3 Security Management of PSI

5.3.1 PII, PSI, secured data, and any other information that must be safeguarded against unauthorized access should be identified and protected. Anyone with access to data resources who is uncertain whether or not it contains PSI or secured data must seek direction from the Data Governance Council, the appropriate data steward or data custodian, the campus HIPAA Privacy Officer, or the University's Chief Information Security Officer (CISO).

5.3.2 Any individual who stores export-controlled patentable research shall have and follow a CISO-approved security plan.

5.3.3 The CISO must approve security procedures for technology assets, which includes any devices, systems, or applications that do not necessarily store, process, or transmit PSI, if access to such resources may cause a breach of security.

5.3.4 Individuals are responsible for ensuring that all electronic information, hard copy information, and hardware devices in their possession are physically protected in accordance with the record classification level as either private or protected data. For more information, (refer to UVU Policy 133 *Compliance with Government Records Access and Management Act* and the *University Data Classification and Encryption Guidelines* on the Dx policy website).

#### 5.4 Operational Control Activities

5.4.1 Authorized Dx personnel shall perform the following processes regularly as operational control activities to ensure proper access and functioning of information systems and technology assets:

5.4.1.1 Assess availability, performance, and capacity of services and resources to ensure that cost-effective capacity and performance are available.

5.4.1.2 Identify important services to the organization, map services and resources to organization processes, and identify key organization dependencies.

5.4.1.3 Plan and prioritize availability, performance, and capacity implications of changing organization needs and service requirements.

5.4.1.4 Continually monitor, measure, analyze, and review availability, performance, and capacity.

5.4.1.5 Investigate and address availability, performance, and capacity issues through monitoring and investigating.

488



# UTAH VALLEY UNIVERSITY

## Policies and Procedures

Page 18 of 42

### 5.5 Required Annual Security Training

5.5.1 The Chief Information Security Officer (CISO) is responsible for developing and maintaining training content as follows:-

5.5.1.1 Training materials must be reviewed and updated at least annually to reflect evolving threats, compliance obligations, and University policies.

5.5.1.2 Updates may also be made in response to security incidents, audit findings, or regulatory changes.

5.5.1.3 The CISO may incorporate external training vendors or tools as needed to ensure quality and relevance.

5.5.1.4 The uUniversity employee learning management system LMS will be used to assign and deliver training annually to all employees.

~~5.4.1.6~~5.5.1.5 Training completion will be tracked automatically through the LMS.

#### POLICY HISTORY

**Date of Last Formal Review:** Click here to enter a date.

**Due Date of Next Review:** Click here to enter a date.

Date of Last Action	Action Taken	Authorizing Entity
October 14, 2004	Policy approved.	UVU Board of Trustees
May 9, 2023	Revised policy approved.	UVU Board of Trustees
	Revised policy approved.	UVU Board of Trustees



# UTAH VALLEY UNIVERSITY

## Policies and Procedures

<b>POLICY TITLE</b>	Information Security	<b>Policy Number</b>	447
<b>Section</b>	Facilities, Operations, and Information Technology	<b>Approval Date</b>	
<b>Subsection</b>	Information Technology	<b>Effective Date</b>	
<b>Responsible Office</b>	Office of the Vice President of Digital Transformation		

### 1.0 PURPOSE

**1.2** The purpose of this policy is to establish the Utah Valley University Information Security Program in compliance with all applicable legal obligations. This program will ensure the protection of university technology assets, information systems, and electronic and digital resources from unauthorized access or damage; and maintain the confidentiality, integrity, and availability of technology assets and information systems supporting the mission and functions of the University.

### 2.0 REFERENCES

- 2.19** *Family Educational Rights and Privacy Act (FERPA)*, 20 U.S.C. § 1232g (1974)
- 2.20** *Federal Information Security Management (FISMA)*, 44 U.S.C. § 3541 (2002)
- 2.21** *American Recovery and Reinvestment Act of 2009*, Pub. L. No. 111-5, 123 stat 115 (2009)
- 2.22** *Offenses Against the Administration of Government*, Utah Code Ann. § 76-8-703 and 705 (2013)
- 2.23** *Interception of Communications Act*, Utah Code Ann. § 77-23a-1 (1980)
- 2.24** *ISO 27002:2022, Information Technology – Security Techniques – Code of Practice for Information Security Management*
- 2.25** *UVU Policy 133 Compliance with Government Records Access and Management Act*
- 2.26** *UVU Policy 135 Use of Copyrighted Materials*
- 2.27** *UVU Policy 241 University Procurement*
- 2.28** *UVU Policy 309 Executive Employees: Recruitment, Compensation, Termination*
- 2.29** *UVU Policy 371 Corrective Actions and Termination for Staff Employees*



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 20 of 42

- 521 ~~2.30 UVU Policy 445 Institutional Data Management and Access~~
- 522 ~~2.31 UVU Policy 446 Privacy and Disclosure~~
- 523 ~~2.32 UVU Policy 448 Authorization and Management of Web, Internet, and Domains~~
- 524 ~~2.33 UVU Policy 451 Retention of Electronic Files~~
- 525 ~~2.34 UVU Policy 457 PCI DSS Compliance~~
- 526 ~~2.35 UVU Policy 541 Student Code of Conduct~~
- 527 ~~2.36 UVU Policy 635 Faculty Rights and Professional Responsibilities~~

### 3.0 DEFINITIONS

- 528 ~~3.34 Account:~~ A login ID which, in combination with a password, PIN, or other authentication  
529 token, is used to access a university information system, digital or electronic resources.
- 530 ~~3.35 Application:~~ An individual or standalone piece of software that is used to provide a  
531 specific service to a community of users or is used as an interface to an information system.
- 532 ~~3.36 Asset:~~ Any university owned information, asset, digital or electronic resources that is a part  
533 of university business processes.
- 534 ~~3.37 Audit log:~~ A chronological sequence of audit records, each of which contains evidence  
535 directly pertaining to and resulting from the execution of a business process or system function.
- 536 ~~3.38 Change:~~ For purposes of this policy, an event or action which modifies the configuration of  
537 any component, application, information system, or service.
- 538 ~~3.39 Confidential information:~~ Any information that is not generally available to the public  
539 and that university has identified as confidential, that should reasonably be understood to be  
540 confidential, or that university is obligated to keep confidential under applicable laws,  
541 regulations, contractual obligations, university policies, or the policies of relevant government  
542 agencies, including but not limited to PII, student records, financial information, research data,  
543 and sensitive information.
- 544 ~~3.40 Control:~~ A means of managing risk, including policies, rules, procedures, processes,  
545 practices, or organizational structures, which can be of administrative, technical, physical,  
546 management, or legal nature. *Control* is also used as a synonym for *safeguard* or  
547 *countermeasure*.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 21 of 42

548 **3.41 Crash:** A disruption of the supervisory or accounting functions of the computing facilities  
549 or doing anything which is likely to have that effect.

550 **3.42 Digital resource:** Any device that is owned by the University or used to conduct university  
551 business regardless of ownership; connected to the University's network; used to create, access,  
552 maintain, or transmit technology assets; or used for the processing, transmitting, or electronic  
553 storage of any data or information. This includes but is not limited to servers, workstations,  
554 mobile devices, medical devices, networking devices, and web cameras or other monitoring  
555 devices.

556 **3.43**

557 **3.44 Disruptive activities:** Acts prohibited by Utah law that interfere with university or student  
558 activities. (See Utah Code Ann. § 76-8-703 to 705.)

559 **3.45 Electronic resource:** Any resource used for electronic communication, including but not  
560 limited to internet, email, and social media.

561 **3.46 Encryption:** The process by which information is altered using a code or mathematical  
562 algorithm to be unintelligible to unauthorized readers.

563 **3.47 Firewall:** A device or program that controls network traffic flow between networks or hosts  
564 that employ disparate security policies.

565 **3.48 Incident:** A confirmed or suspected security breach.

566 **3.49 Incident Response Team:** Directed by the Chief CISO) and made up of campus personnel;  
567 the Incident Response Team is responsible for immediate response to any breach of security.  
568 One or more members of the Incident Response Team must be technically qualified to respond to  
569 information-related incidents. The Incident Response Team is also responsible for determining  
570 and disseminating remedies and preventive measures that develop as a result of responding to  
571 and resolving security breaches.

572 **3.50 Information asset:** Data or knowledge stored in any electronic manner and recognized as  
573 having value for the purpose of enabling the University to perform its business functions.

574 **3.51 Information security incidents:** Events or weaknesses that jeopardize the confidentiality,  
575 integrity, and availability of the University's technology assets, digital or electronic resources,  
576 and information systems.

577 **3.52 Information system:** An application or group of servers used for the electronic storage,  
578 processing, or transmitting of any university data or information asset.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 22 of 42

**3.53 Information system media:** Physical media on which an information system's technology assets are stored for backup and recovery purposes (e.g., backup tapes, backup disks, NAS/SAN drives, magnetic media, etc.).

**3.54 Intellectual property:** Any intangible asset that consists of human knowledge and ideas (e.g., patents, copyrights, trademarks, software, etc.).

**3.55 IT technicians:** Individuals who develop, administer, manage, and monitor the information systems, and digital or electronic resources that support the University's IT infrastructure. These individuals are responsible for the security of the IT resources, information systems, and electronic resources they manage, and IT technicians assure that security-related activities are well documented and completed in a consistent and auditable manner.

**3.56 Patch:** A fix to a program failure, bug, or vulnerability. A patch may also be referred to as a Service Pack.

**3.57 Personally identifiable information (PII):** Unique identifiers, including a person's Social Security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, and personal email addresses.

**3.58 Private Sensitive Information (PSI):** Social security numbers, credit card information, health, and medical records, financial records, that give specific information about an individual that is considered private or sensitive and can lead to adverse consequences if disclosed, such as identity theft, financial loss, or invasion of privacy. Access to such data is governed by state and federal laws, both in terms of protection of the data, and requirements for disclosing the data to the individual to whom it pertains. It does not include "public information" as defined by GRAMA or directory information as defined by FERPA.

**3.59 Risk:** The likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. Risk is usually calculated as either a quantitative or qualitative score and can be represented in the following equation:  $\text{Risk} = (\text{likelihood of threat/vulnerability event occurrence}) \times (\text{business impact of event occurring})$ .

**3.60 Routine maintenance of the system:** Includes but is not limited to security checks, deletion of temporary files, verification of email delivery, and assurance of available disk space.

**3.61 Security breach:** Includes but is not limited to unauthorized use of an account, unauthorized access or unauthorized changes to system resources, use of bad passwords, or attempted use or acquisition of others' passwords.

**3.62 Security check:** Verification that privacy is ensured and access is granted as needed and appropriate.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 23 of 42

**3.63 Server:** Hardware, software, and workstations used to provide information and services to multiple users.

**3.64 System files:** Any files that control or otherwise affect the startup or operation of a computer system.

**3.65 Unauthorized access:** Obtaining access into any digital or electronic resource, network, storage medium, system, program, file, user area, controlled physical area, or other private repository without the permission of the steward or owner.

**3.66 User:** Any person who accesses any university information systems and digital and electronic resources, including students, staff, faculty, permanent and temporary employees, contractors, vendors, research collaborators, and third-party agents.

**3.67 Vulnerability:** A weakness that could be used to endanger or cause harm to an asset.

**3.68 Workstation:** An electronic computing device, terminal, or any other device that performs as a general purpose computer equipped with a microprocessor and designed to run commercial software (such as a word processing application or internet browser) for an individual user (e.g., laptop, desktop computer, PC, Mac, etc.).

## 4.0 POLICY

### 4.23.14.22 Scope of this Policy

4.23.14.22.1 Compliance with this policy and all its related procedures is required for all university administrative units, including colleges, divisions, departments, and centers and all members of the university community, including students, staff, faculty, other permanent or temporary employees, contractors, research collaborators, vendors, and third-party agents. This policy applies to anyone in the university community owning or overseeing the use of any type of computing device connected to the UVU network, including but not limited to:

4.23.1.14.22.1.1 UVU department heads, even in cases where vendor-owned or vendor-managed equipment is housed in departments; and

4.23.1.24.22.1.2 Faculty, staff, students, and other individuals who have devices connected to the UVU network, even if those devices were acquired personally, i.e., not with university or grant funds; and

4.23.1.34.22.1.3 Digital Transformation (Dx) for the enterprise IT devices under ongoing support contracts.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 24 of 42

644 ~~4.23.24.22.2~~ If no one claims responsibility for a device, the UVU department head for the  
645 department in which the device resides shall be presumed to be responsible by default.

646 ~~4.23.34.22.3~~ This policy applies to individuals responsible (as defined above) for devices that  
647 serve more than one user and to those responsible for single user devices.

648 ~~4.23.44.22.4~~ When devices are used for university business, compliance shall be verified by  
649 Internal Audit during routine audits.

#### 650 ~~4.24.23~~ User Responsibilities

651 ~~4.24.14.23.1~~ Use of the UVU technology assets must be legal, ethical, and consistent with the  
652 University's mission. User violations of this policy may reflect negatively on the University.

653 ~~4.24.24.23.2~~ Instructional, administrative, and research uses of system resources take priority  
654 over all other uses.

655 ~~4.24.34.23.3~~ Individual users shall do the following:

656 ~~4.24.3.14.23.3.1~~ Maintain the security and confidentiality of confidential information assets; and

657 ~~4.24.3.24.23.3.2~~ Exercise caution in the storage and disposal of files containing confidential  
658 information assets; and

659 ~~4.24.3.34.23.3.3~~ Choose safe passwords, change them often, and do not disclose them; and

660 ~~4.24.3.44.23.3.4~~ Backup all private, important, or irreplaceable files, and regularly perform  
661 personal file maintenance (including scanning for viruses and sensitive data and deleting  
662 unnecessary files); and

663 ~~4.24.3.54.23.3.5~~ Ascertain and understand the laws, policies, rules, procedures, contracts, and  
664 licenses applicable to their particular uses; and

665 ~~4.24.3.64.23.3.6~~ Comply with all federal, state, and other applicable laws, all generally  
666 applicable university regulations, and all applicable contracts and licenses; and

667 ~~4.24.3.74.23.3.7~~ Use only those university information systems and digital and electronic  
668 resources that they are authorized to use and use them only in the manner and to the extent  
669 authorized; and

670 ~~4.24.3.84.23.3.8~~ Refrain from unauthorized attempts to circumvent the security mechanisms of  
671 any university digital or electronic resource; and





## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 25 of 42

672 ~~4.24.3.94.23.3.9~~ Refrain from attempts to degrade system performance or capabilities or damage  
673 digital or electronic resources information systems, software, or intellectual property of others;  
674 and

675 ~~4.24.3.104.23.3.10~~ Use multi-factor authentication required for all administrative and functional  
676 access to digital or electronic resources that store, process, or transmit personally identifiable  
677 information.

678 ~~4.24.3.114.23.3.11~~ Immediately report any suspected or actual security breach to the University's  
679 Information Security Office (ISO), the appropriate data steward, and data custodian.

680 ~~4.24.44.23.4~~ Employees are required to follow current IT standards and controls for safeguarding  
681 against electronically stored PSI. UVU should not use an individual's Social Security Number  
682 (SSN) or Driver's License Number (DLN) as a personal identifier except as required by law.  
683 Restricted information, including SSNs and DLNs, may be stored electronically only in  
684 compliance with current IT standards. If restricted information must be stored on paper, the files  
685 must be stored securely with access provided only to authorized persons.

686  
687 ~~4.24.54.23.5~~ All data users having access to legally restricted or limited access data shall  
688 formally acknowledge (by signed statement or some other means) their understanding of the  
689 level of access provided and their responsibility to maintain the confidentiality of data they  
690 access. Each data user shall be responsible for the consequences of any misuse, including  
691 intentional misrepresentation of institutional data.

#### 692 ~~4.254.24~~ User Prohibitions

693 ~~4.25.14.24.1~~ Users shall not do the following:

694 ~~4.25.1.14.24.1.1~~ Share passwords or accounts; or

695 ~~4.25.1.24.24.1.2~~ Copy or change system files or software without authorization from a system  
696 administrator; or

697 ~~4.25.1.34.24.1.3~~ Consume inordinate amounts of system resources (e.g., disk space, CPU time,  
698 email system, printing facilities, and dial-up access lines), as determined by affected system  
699 administrators; or

700 ~~4.25.1.44.24.1.4~~ Crash machines or systems recklessly or deliberately; or

701 ~~4.25.1.54.24.1.5~~ Lock a public shared technology asset without authorization from a supervisor  
702 or asset manager; or

703 ~~4.25.1.64.24.1.6~~ Use the university technology assets for disruptive or illegal activities; or



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 26 of 42

~~4.25.1.74.24.1.7 Violate licensing agreements; patent, copyright, or trademark laws; or UVU Purchasing regulations as governed by UVU Policy 241 *University Procurement*; or~~

~~4.25.1.84.24.1.8 Reserve shared resources. A public shared computing facility device left unattended for more than ten minutes is available for use, and any process running at the time of abandonment shall be terminated. Running unattended programs or placing signs on devices to “reserve” them during a user’s absence is inappropriate without authorization from a system administrator or lab assistant; or~~

~~4.25.1.94.24.1.9 Use weak passwords. Users shall not use easily guessable passwords. Weak passwords can create security breaches, and failure to change a weak password when directed by a system administrator to do so will result in a locked account. Examples of weak passwords include~~

- ~~• Information related to the user (such as phone number, birth date, license plate number, spouse name, etc.); or~~

- ~~• Dictionary words in any language, or phrases from books, films, poems, songs (song lyrics), famous speeches, etc.; or~~

- ~~• Words with simple algorithms applied, such as using the same word backwards, concatenating two words, or concatenating two words with a punctuation character in between (e.g., Elponitnatsnoc, yenoh, eipragus, yellowtiger, regitwolley, cat?dog, star!search).~~

~~4.25.24.24.2 Unless specifically approved by the Data Governance Council and registered with University's Information Security Office (ISO) according to the procedures below, anyone given access to university data shall not electronically transmit or knowingly retain on personal computers, servers, or computing or storage devices any PSI.~~

#### ~~4.264.25 System Administrator Rights and Responsibilities~~

~~4.26.14.25.1 System administrators must perform routine maintenance of the system and keep a backup of information. System administrators are not responsible for data lost due to system errors.~~

~~4.26.24.25.2 Dx, including system administrators, shall work in partnership with data owners and data stewards in fulfilling the responsibilities outlined in this policy.~~

#### ~~4.274.26 Intellectual Property Use~~

~~4.27.14.26.1 All users of intellectual property shall comply with UVU Policy 136 *Intellectual Property*, including refraining from~~



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 27 of 42

~~4.27.1.14.26.1.1~~ Installing or distributing "pirated" or other software products that are not appropriately licensed for use by the University; and

~~4.27.1.24.26.1.2~~ Violating the rights of any person or company protected by trade secret, patent, or any other intellectual property laws or similar laws or regulations.

#### ~~4.28.4.27~~ **Data Classification and Encryption**

~~4.28.14.27.1~~ The University shall take measures to protect university technology assets that are created, maintained, processed, or transmitted using information systems and digital or electronic resources. These measures shall be implemented commensurate with the assessed level of risk and reviewed at regular intervals.

~~4.28.24.27.2~~ IT technicians are primarily responsible for establishing, documenting, implementing, and managing data handling and management procedures for the information and digital or electronic resources systems they support.

~~4.28.34.27.3~~ All technology assets shall be classified in accordance with the *Data Classification and Encryption Guideline*, which can be found on the Office of Information Technology IT policies website.

~~4.28.44.27.4~~ All technology assets shall have appropriate data handling procedures in accordance with the data classification.

~~4.28.54.27.5~~ All technology assets shall have encryption requirements in accordance with the *Data Classification and Encryption Guideline*, which can be found on the Office of Information Technology IT policies website.

#### ~~4.29.4.28~~ **Information Security Risk and Threat Management**

~~4.29.14.28.1~~ The University's Information Security Risk Management Program shall support the University's business missions while also mitigating financial, operational, reputational, and regulatory compliance risk. Appropriate risk management enables the University to accomplish its mission by doing the following:

~~4.29.1.14.28.1.1~~ Securing the information systems that create, maintain, process, or transmit the University's technology assets; and

~~4.29.1.24.28.1.2~~ Enabling the appropriate university personnel to make well informed decisions regarding risk and risk management; and

~~4.29.1.34.28.1.3~~ Collaborating with other university risk management activities to ensure the University's information security program priorities are aligned appropriately with the University's risk tolerance; and



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 28 of 42

~~4.29.1.44.28.1.4~~ Providing a systematic methodology to assess and manage information security risk for the University; and

~~4.29.1.54.28.1.5~~ Reviewing contracts and terms of service to ensure that third parties entrusted with personally identifiable information will implement reasonable protections for that information in all stages of its lifecycle including creation, storage, processing, recovery, transmittal, and destruction.

~~4.29.24.28.2~~ Information systems and digital or electronic resources shall be protected commensurate with the assessed level of risk, and security baseline settings shall be utilized to ensure these systems and resources are guarded against malware and available for use. All IT technicians, IT personnel, and users managing university information systems and digital or electronic resources shall do the following:

~~4.29.2.14.28.2.1~~ Protect any information systems and digital or electronic resources under their management from compromise; and

~~4.29.2.24.28.2.2~~ Ensure the products and services provided continue to be delivered at acceptable levels during a disruptive incident. Incidents may be caused by problems with IT, telephones, the building, or external environment (such as weather); and

~~4.29.2.34.28.2.3~~ Configure information systems and digital or electronic resources to reduce vulnerabilities to an acceptable risk level; and

~~4.29.2.44.28.2.4~~ Install anti-virus or other anti-malware tools, install relevant security patches, and implement security best practices for digital or electronic resources; and

~~4.29.2.54.28.2.5~~ Periodically verify audit and activity logs, examine performance data, and check for any evidence of unauthorized access, viruses, or other malicious code; and

~~4.29.2.64.28.2.6~~ Cooperate with the Information Security Office by providing support for and review of administrative activities as well as performing more sophisticated procedures such as penetration testing (also called pen testing or ethical hacking) to test a computer system, network, or web application to find security vulnerabilities that an attacker could exploit along with real-time intrusion detection.

#### ~~4.304.29~~ Access Management

~~4.30.14.29.1~~ Only authorized users shall have physical, electronic, or other access to information systems, technology assets, and digital or electronic resources. Access shall be limited to users with a business need to know and limited only to the requirements of their job function. It is the shared responsibility of IT technicians and users to prevent unauthorized access to these resources. Access controls shall include prevention and detection of unauthorized use, and



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 29 of 42

801 effective procedures for granting authorization, tools, and practices to authenticate authorized  
802 users.

803 [4.30.24.29.2](#) The appropriate university system administration group shall issue university  
804 accounts after the request is authorized appropriately and documented adequately.

805 [4.30.34.29.3](#) The appropriate university system administration group shall authenticate university  
806 accounts at a minimum via unique login and complex passwords.

807 [4.30.44.29.4](#) The appropriate university system administration group shall deactivate, disable, or  
808 delete university accounts—except where maintaining such accounts is a business necessity—as  
809 soon as reasonably possible after receiving authorized notification of termination of contract,  
810 employment, or relationship with the University.

811 [4.30.54.29.5](#) The appropriate university security group shall conduct periodic reviews of  
812 authorized access commensurate with the assessed level of risk.

#### 813 [4.314.30](#) **Change Management**

814 [4.31.14.30.1](#) Any changes to university production information systems and digital or electronic  
815 resources that store, process, transmit, or maintain confidential data shall be authorized, tested,  
816 documented, and approved prior to implementation. Digital Transformation will notify the  
817 affected entities.

#### 818 [4.324.31](#) **Physical and Facility Security**

819 [4.32.14.31.1](#) University IT resources and information systems shall be physically protected  
820 commensurate with the assessed level of risk. IT technicians and personnel shall ensure that  
821 controls are planned and implemented for safeguarding physical components against  
822 compromise and environmental hazards. Locks, cameras, alarms, redundant power systems, fire  
823 detection and suppression systems, and other safeguards as appropriate shall be installed in data  
824 centers and technology closets to ensure protection from natural and facility threats and to  
825 discourage and respond to unauthorized access to electronic or physical components contained in  
826 these areas.

827 [4.32.24.31.2](#) The institution shall maintain an inventory of all internal or third-party digital or  
828 electronic resources that store, process, or transmit personally identifiable information.

#### 829 [4.334.32](#) **Remote Access**

830 [4.33.14.32.1](#) Users with remote access privileges to any of the University's networks inside a  
831 firewall must connect through an approved connection method such as a secure VPN.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 30 of 42

~~4.33.24.32.2~~ Users with remote access privileges to the University's digital or electronic resources must ensure that all devices being used are given the same security considerations as outlined in the IT security annual training. Specific security questions should be directed to the IT Security Department.

#### ~~4.34.33~~ Network Security

~~4.34.14.33.1~~ Access to both internal and external networked services shall be controlled and protected commensurate with the assessed level of risk. User, information system and digital or electronic access to networks and network services shall not compromise the security of the network services by ensuring the following:

~~4.34.1.14.33.1.1~~ Appropriate controls are in place between the University's network, networks owned by other organizations, and public networks; and

~~4.34.1.24.33.1.2~~ Appropriate authentication mechanisms are applied for users, information systems and digital or electronic resources.

#### ~~4.35.34~~ Log Management and Monitoring

~~4.35.14.34.1~~ The appropriate IT personnel, in coordination with the ISO, shall configure university information systems and digital or electronic resources to record and monitor information security incidents, events and weaknesses. They shall regularly review and analyze audit logs for indications of inappropriate or unusual activity.

#### ~~4.36.35~~ Information System Media Handling

~~4.36.14.35.1~~ University information system media shall be inventoried, controlled, and physically protected commensurate with the assessed level of risk and the *Data Classification and Encryption Guideline* to prevent interruption to business activities or unauthorized disclosure, modification, removal, or destruction of technology assets. Appropriate operating procedures shall be established to protect information system media, input/output data, and system documentation from unauthorized disclosure, modification, removal, and destruction.

~~4.36.24.35.2~~ The appropriate university system administration or security group shall restrict access to information system media to authorized individuals.

~~4.36.34.35.3~~ All institutionally owned computing devices, including removable storage devices, shall have industry standard encryption that renders the storage media of those devices reasonably unrecoverable by a third party or shall implement other reasonable controls.

~~4.36.44.35.4~~ The University shall physically control and securely store information system media on-site within controlled areas where appropriate and ensure any authorized off-site storage is, at minimum, secured at the same level as the on-site area.





## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 31 of 42

~~4.36.54.35.5~~ The University shall protect and control information system media during transport outside of controlled areas and shall restrict the activities associated with transport of such media to authorized personnel.

~~4.36.64.35.6~~ The University shall sanitize or destroy information system media containing confidential data prior to disposal or release for reuse in accordance with National Institute of Standards and Technology guidance.

#### ~~4.374.36~~ **Future Technology Needs Assessment**

~~4.37.14.36.1~~ IT shall ensure current and future needs for availability, performance, and capacity with cost-effective service provision. This includes assessment of current capabilities, future needs based on organization requirements, and implementation of actions to meet the new requirements. The goal is to ensure service availability, efficient management of resources, and optimization of system performance through effective capacity planning.

#### ~~4.384.37~~ **Information Security Awareness and Training**

~~4.38.14.37.1~~ All university employees and other affiliates are required to complete appropriate security training relevant to their roles and responsibilities before gaining access to systems, records, and information resources and shall renew that training annually. If university employees and other affiliates do not fulfill these training requirements, their access may be subject to revocation.

~~4.38.24.37.2~~ The appropriate university information systems and security groups shall stay up to date with the latest recommended security practices, techniques, and technologies, and the latest security-related information including threats, vulnerabilities, and incidents.

#### ~~4.394.38~~ **Internal Audit Assessment**

~~4.39.14.38.1~~ Internal Audit shall audit systems used for university business to ensure compliance with this policy and industry security standards.

#### ~~4.404.39~~ **Violations**

~~4.40.14.39.1~~ Incidents of actual or suspected non-compliance with this policy or associated regulations must be reported to the Information Security Office, whose administrators will work with the appropriate authorities to resolve the issue.

~~4.40.24.39.2~~ The University reserves the right to revoke access to any resource for any user who violates this policy or associated regulations or for any other business reasons in conformance with applicable policies. Violations of this policy or associated regulations may result in other disciplinary action in accordance with pertinent university policies.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 32 of 42

897 **4.414.40 Security Standards**

898 **4.41.14.40.1** ~~Those responsible for devices connected to the UVU network must ensure that key~~  
899 ~~security vulnerabilities are eliminated from these devices.~~

900 **4.41.24.40.2** ~~Dx shall maintain and communicate to device owners a current list of key~~  
901 ~~vulnerabilities and steps required to mitigate the vulnerabilities. Device owners are responsible~~  
902 ~~for addressing those vulnerabilities promptly with IT assistance as needed.~~

903 **4.424.41 Enforcement**

904 **4.42.14.41.1** ~~In cases where university network resources and privileges are threatened by~~  
905 ~~improperly maintained computing devices, OIT may eliminate the threat, working with the~~  
906 ~~relevant device owner where possible. This may include denial of access to campus resources.~~

907 **4.434.42 Exceptions to Policy**

908 **4.43.14.42.1** ~~Exceptions to this policy must be justified, approved, and reviewed annually as~~  
909 ~~outlined in the procedures. Requests for exceptions to this policy shall be made in writing to the~~  
910 ~~Chief Information Officer. Exception may be granted if the benefits to the University far~~  
911 ~~outweigh the risks of the vulnerable device, as judged by the Chief Information Officer.~~

912 **4.444.43 Review and Maintenance of Policy**

913 **4.44.14.43.1** ~~The IT Oversight Committee, including the Chief Information Officer, shall review~~  
914 ~~this policy at least annually and evaluate changes in law and technology that may impact the~~  
915 ~~University. The committee shall invite representatives of UVUSA, PACE, General Counsel, and~~  
916 ~~Faculty Senate to participate.~~

## 5.0 PROCEDURES

917 **5.55.6 Physical Security of Enterprise Hardware**

918 **5.5.15.6.1** ~~Any department that assumes responsibility for administrative data must ensure that~~  
919 ~~the computing systems housing the data are physically secure. Areas to address include the~~  
920 ~~following:~~

921 1) ~~The equipment shall be protected from excessive heat, cold, humidity, and dryness. Alarms~~  
922 ~~shall exist to warn of thresholds being exceeded; and~~

923 2) ~~The equipment shall be protected against electrical interruptions, voltage spikes, and surges;~~  
924 ~~and~~





## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 33 of 42

- 925 3) The equipment shall be protected with smoke detectors, fire extinguishers, and air-tight  
926 computer rooms for containment of fire suppression gas, air filters, and water sensors. Alarms  
927 tied to the University and city police departments shall be installed; and
- 928 4) The equipment shall be properly locked up with no vulnerabilities from drop ceilings, raised  
929 floors, or ventilation ducts. A log of accesses by personnel shall be kept; and
- 930 5) Backups shall be moved offsite, and a fireproof vault shall be used if backups remain onsite.  
931 The offsite storage location shall be securely maintained and managed in a manner appropriate  
932 for the storage of university data; and
- 933 6) The history of theft and vandalism in the buildings of the immediate vicinity shall be  
934 considered, and appropriate measures shall be taken to counteract the risks; and
- 935 7) A disaster recovery plan shall exist, and drills shall be conducted on a regular basis. Offsite  
936 documentation shall exist, and key personnel shall be cross-trained to handle an emergency.
- 937 5.5.25.6.2 Owners of devices shall install and run campus approved anti-virus software on these  
938 devices and apply updates from the software vendor as they become available.
- 939 5.5.35.6.3 Owners of devices shall apply security-related updates to the operating system  
940 running on their devices as these updates become available from operating system vendors.
- 941 5.5.45.6.4 Owners of devices shall switch off unneeded services or use a firewall to eliminate the  
942 risk of these being exploited.
- 943 5.65.7 **Incident Management**
- 944 5.6.15.7.1 All suspected or actual security breaches of university or departmental systems must  
945 be reported immediately to the University's Chief Information Security Office (CISO). (Reports  
946 may be emailed to SECURITY@UVU.EDU.) The incident must also be reported to the  
947 appropriate data steward and data custodian.
- 948 5.6.25.7.2 If the compromised system contains PII or PSI as outlined in UVU Policy 445  
949 *Institutional Data Management and Access*, IT personnel or the appropriate data owner must  
950 report the incident to the Office of General Counsel. Additional technical, forensic, and other  
951 support may be sought from outside the campus community.
- 952 5.6.35.7.3 If PII, PSI, secured data, or any other information that must be safeguarded against  
953 unauthorized access has been accessed or compromised by unauthorized persons or  
954 organizations, IT personnel or the appropriate data owner must report the incident immediately  
955 to the ISO (SECURITY@UVU.EDU) and cooperate with their dean, department head, or  
956 supervisor; the Incident Response Team; their respective vice president; and the Office of  
957 General Counsel to assess the level of threat or liability posed to the University and to those



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 34 of 42

whose PSI was accessed. In accordance with applicable laws, the University shall notify the individuals whose PSI was accessed or compromised, providing them with instructions regarding measures to be taken to protect themselves from identity theft.

#### **5.75.8 Security Management of PSI**

**5.7.15.8.1** PH, PSI, secured data, and any other information that must be safeguarded against unauthorized access should be identified and protected. Anyone with access to data resources who is uncertain whether or not it contains PSI or secured data must seek direction from the Data Governance Council, the appropriate data steward or data custodian, the campus HIPAA Privacy Officer, or the University's Chief Information Security Officer (CISO).

**5.7.25.8.2** Any individual who stores export-controlled patentable research shall have and follow a CISO approved security plan.

**5.7.35.8.3** Security procedures must be approved by the CISO for any devices or systems that do not necessarily store, process, or transmit PSI, if access to such resources may cause a breach of security.

**5.7.45.8.4** Individuals are responsible for ensuring that all electronic information, hard copy information, and hardware devices in their possession are physically protected in accordance with the record classification level as either private or protected data. For more information, (refer to UVU Policy 133 *Compliance with Government Records Access and Management Act* and the *University Data Classification and Encryption Guidelines*).

#### **5.85.9**

#### **5.95.10 Control Activities**

**5.9.15.10.1** Authorized Dx personnel shall perform the following processes regularly as control activities:

1) Assess availability, performance, and capacity of services and resources to ensure that cost-effective capacity and performance are available; and

2) Identify important services to the organization, map services and resources to organization processes, and identify key organization dependencies; and

3) Plan and prioritize availability, performance, and capacity implications of changing organization needs and service requirements; and

4) Continually monitor, measure, analyze, and review availability, performance, and capacity; and



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 35 of 42

989 5) Investigate and address availability, performance, and capacity issues through monitoring and  
990 investigating.



## POLICY 447 EXECUTIVE SUMMARY

**Policy Number and Title:** 447 Information Security

<b>Date:</b>	April 29, 2024
<b>Sponsor:</b>	Christina Baum
<b>Steward(s):</b>	Brett McKeachnie
<b>Policy Process:</b>	Regular
<b>Policy Action:</b>	Revision
<b>Policy Office Editor:</b>	Cara O'Sullivan
<b>Embedded Attorney:</b>	James Duncan

### Issues/Concerns (including fiscal, legal, and compliance impact):

We decided it was appropriate to move language addressing Private Sensitive Information to this policy. This policy update does not make any significant changes to the rest of the policy or its purpose nor intent.

### Suggested Changes:

Revisions are inserting relevant Private Sensitive Information material, the definition, and procedures to be contained in this policy so that Policy 449 Private Sensitive Information can be deleted.

**Requested Approval from President's Council:** Entrance to Stage 1

**Proposed Drafting Committee:** Joe Belnap, LeRoy Brown, Brett McKeachnie, others TBD

**Target Date for Stage 1 Draft to Enter Stage 2:** 8/19/2024

**Target Date for Board of Trustees Review:** 10/31/2024



# UTAH VALLEY UNIVERSITY

## Policies and Procedures

Page 37 of 42

### EQUITY ASSESSMENT COMMITTEE (EAC) FORM

**Policy Number and Title:** 447 Information Security

**Sponsor:** Christina Baum  
**Steward(s):** Brett McKeachnie  
**EAC Review:** March 6, 2025  
**Owner Review:** TBD

**UVU Scope (Groups Impacted):**

Adult learners	Pregnancy, pregnancy-related conditions
Age (40+)	Race and ethnicity
Color	Religion, spirituality, and worldviews
First-generation student status	Sex, gender identity, and gender expression
Individuals with apparent or non-apparent disabilities	Sexual orientation
National origin and citizenship status	Socioeconomic status
	Veteran status (including uniformed military status)

*Note: This form is for internal use only by the EAC and policy owners (sponsors, stewards, and coordinators). This form captures general equity concerns and those that impact the specific groups listed. This form will accompany the Stage 2 draft.*

Section	Groups Impacted	General Equity	Equity Concern	Recommendation	Policy Owner Proposed Solution
			No concerns.		



# UTAH VALLEY UNIVERSITY

## Policies and Procedures

SUMMARY OF COMMENTS (STAGE 2)			
<b>Policy Number and Title:</b> 447 <i>Information Security</i>			
<b>Sponsor:</b> Christina Baum			
<b>Steward(s):</b> Brett McKeachnie			
<b>UVUSA</b>	<b>Academic Affairs</b>	<b>Faculty Senate</b>	<b>PACE</b>
Date Presented: _____	Date Presented: _____	Date Presented: _____	Date Presented: _____

*Note: Indicate with X whether the comment is editorial (grammar, punctuation, sentence structure) or is a substance comment (content, procedure, etc.)*

Campus Entity	Policy Section	Editorial Comment	Substance Comment	Concern	Sponsor/Steward Response
PACE	Overall		X	Policy 449 mentioned “screen and computer locks, and making screen displays or physical storage devices unavailable to unauthorized personnel.” But that is not included in 447. Intentional? Easiest way to breach security is human error, which includes not locking a screen.	Thank you. We have added a new section 4.2.3.5 with the requirement to configure automation for and to lock screens during periods of inactivity.



## UTAH VALLEY UNIVERSITY

### Policies and Procedures

Page 39 of 42

PACE	4.3.2		X	<p>Please add some language on who to contact with questions on if data is PSI and/or what security requirements are required. For example, referencing 5.3.1.</p> <p>5.3.1 is great information but kind of hidden and unclear if someone is specifically looking for who to contact.</p>	<p>Thank you. We have added a reference in 4.3.2 directing readers to procedure 5.3.1.</p>
PACE	4.6.5		X	<p>There is confusion from staff on how to identify encryption requirements, who to contact if encryption is needed, and what they need to do to get that process started.</p> <p>For example, the Data Classification and Encryption Guideline does not provide any direction on who to contact with questions or implementation of encryption requirements.</p>	<p>Thank you. We will update the Data Classification and Encryption Guideline to include contact information for support on encryption.</p>
UVUSA	Overall		x	<p>Overall evaluation and take out any overlap to make it more consolidated</p>	<p>We are aware that the many consolidations of security-related policies into this one have made it longer and more complex than is optimal. In our next (annual) review of this policy, we will make it a point to work to simplify and make it as concise as prudent, given the sensitive nature of the</p>



# UTAH VALLEY UNIVERSITY

## Policies and Procedures

Page 40 of 42

					topics covered. At that time, we will also work to move detailed guidelines and procedures to appropriate external documents.
AAC	All		X	<p>Policy length:</p> <p>Recommend condensing the policy, as its current length of 18 pages. This does not seem to be user-friendly to stakeholders. Consider streamlining the content by focusing on essential policy elements while moving detailed guidelines and procedures to an external reference document. The policy should then reference this external document to ensure stakeholders can easily access the necessary details.</p>	<p>We are aware that the many consolidations of security-related policies into this one have made it longer and more complex than is optimal. In our next (annual) review of this policy, we will make it a point to work to simplify and make it as concise as prudent, given the sensitive nature of the topics covered. At that time, we will also work to move detailed guidelines and procedures to appropriate external documents.</p>
AAC	All	X		<p>Readability:</p> <p>For the larger sections, recommend using subheadings with clear titling to make the information more user friendly and accessible to stakeholders.</p>	<p>Noted. In our next (annual) review of this policy, we will make it a point to work to simplify and make it as concise and readable as possible.</p>
AAC	4.5		X	<p>Needed information:</p> <p>This section may not be needed, as it seems to simply refer to UVU Policy 136. Recommend removing.</p>	<p>This section provides specific policy statements related to information</p>





# UTAH VALLEY UNIVERSITY

## Policies and Procedures

Page 41 of 42

					security that are not covered in Policy 136.
AAC	4.15		X	<p>Needed information:</p> <p>This section seems more like an operational strategy, rather than a policy requirement. Is Dx responsible for conducting capacity planning? If not, recommend removing.</p>	<p>The section title limits the scope of the capacity planning (and other requirements for Dx) to technology. Rather than operational strategy, this section requires Dx to ensure that availability, performance, and capacity do not impact the security of systems that support the University's operations.</p>
AAC	4.16.2		X	<p>Clarity needed:</p> <p>What is the training? Who provides it? Is it part of new employee onboarding? Is it completed once, or is it a regularly occurring activity?</p>	<p>We have added section 5.5 to describe the training procedures. We also updated language in 4.16.2 to clarify the intent of remaining current for systems and security personnel. → "The relevant university information systems and security teams shall monitor developments in recognized security practices, methodologies, and technologies, as well as maintain awareness of emerging threats, vulnerabilities, and security incidents."</p>
AAC	4.17		X	<p>Needed information:</p> <p>This section does not seem to be needed in this policy. This is an action that the Office of Internal Audit can do on any</p>	<p>Thank you. We have removed this legacy section from the policy draft.</p>



# UTAH VALLEY UNIVERSITY

## Policies and Procedures

Page 42 of 42

				administrative unit or process within UVU.	
AAC	4.18		X	Accuracy of information: Why would violations not go to EthicsPoint? If another pipeline is created, then the university will not be centrally receiving these reports. Recommend removing.	Due to the sensitive and urgent nature of information security violations, we use an alternative reporting method instead of EthicsPoint, which can introduce delays in response. However, once the immediate issue is addressed, security personnel ensure the incident is reported through central channels for proper documentation and tracking.
AAC	5.2		X	Information inclusion: Should email addresses be included in policy?	Email addresses of individual employees should not be included; email addresses of departments are appropriate.
Faculty Senate				No comments.	