POLICY TITLE	Information Security	**Policy Number**	447
Section	Facilities, Operations, and Information Technology	**Approval Date**	May 9, 2023
Subsection	Information Technology	**Effective Date**	May 9, 2023
Responsible Office	Office of the Vice President of Digital Transformation		

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, information systems, and IT 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

2.1 *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 ISO 27002:2022, *Information Technology - Security Techniques - Code of Practice for Information Security Management*

2.7 UVU Policy 135 *Use of Copyrighted Materials*

2.8 UVU Policy 241 *University Procurement*

2.9 UVU Policy 309 *Executive Employees: Recruitment, Compensation, Termination*

2.10 UVU Policy 371 *Corrective Actions and Termination for Staff Employees*

2.11 UVU Policy 445 *Institutional Data Management and Access*

2.12 UVU Policy 446 *Privacy and Disclosure*

2.13 UVU Policy 448 *Authorization and Management of Web, Internet, and Domains*

2.14 UVU Policy 457 *PCI DSS Compliance*

2.15 UVU Policy 541 *Student Code of Conduct*

2.16 UVU Policy 635 *Faculty Rights and Professional Responsibilities*

3.0 DEFINITIONS

3.1 Account: A login ID which, in combination with a password, PIN, or other authentication token, is used to access a university information system, electronic resource, or IT resource.

3.2 Application: An individual or standalone piece of software that is used to provide a specific service to a community of users or is used as an interface to an information system.

3.3 Asset: Any university-owned information, asset, or IT resource that is a part of university business processes.

3.4 Audit log: A chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

3.5 Change: For purposes of this policy, an event or action which modifies the configuration of any component, application, information system, or service.

3.6 Confidential information: Any information that is not generally available to the public and that university has identified as confidential, that should reasonably be understood to be confidential, or that university is obligated to keep confidential under applicable laws, regulations, contractual obligations, university policies, or the policies of relevant government agencies, including but not limited to PII, student records, financial information, research data, and sensitive information.

3.7 Control: A means of managing risk, including policies, rules, procedures, processes, practices, or organizational structures, which can be of administrative, technical, physical, management, or legal nature. *Control* is also used as a synonym for *safeguard* or *countermeasure*.

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

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

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

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 device or program that controls network traffic flow between networks or hosts that employ disparate security policies.

3.13 Incident: A confirmed or suspected security breach.

3.14 Incident Response Team: Directed by the Information Security Officer (ISO) 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 recognized as having value for the purpose of enabling the University to perform its business functions.

3.16 Information security incidents: Events or weaknesses that jeopardize the confidentiality, integrity, and availability of the University's technology assets, IT resources, and information systems.

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

3.18 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.).

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

3.20 IT technicians: Individuals who develop, administer, manage, and monitor the IT resources, information systems, and 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.

3.21 IT resource: Any device that is owned by the University or 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, mobile devices, medical devices, networking devices, and web cameras or other monitoring devices.

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

3.23 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.

3.24 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: Risk = (likelihood of threat/vulnerability event occurrence) X (business impact of event occurring).

3.25 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.

3.26 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.

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

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

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

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

3.31 User: Any person who accesses any university electronic resources, information systems, or IT resources, 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: 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

4.1 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 computing device connected to the UVU network, including but not limited to:

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

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

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 UVU department head 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 devices that serve more than one user and to those responsible for single-user devices.

4.1.4 When devices are used for university business, compliance shall be verified by Internal Audit during routine audits.

4.2 User Responsibilities

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

4.2.2 Instructional, administrative, and research uses of system resources take priority over all other uses.

4.2.3 Individual users shall do the following:

1) Maintain the security and confidentiality of confidential information assets; and

2) Exercise caution in the storage and disposal of files containing confidential information assets; and

3) Choose safe passwords, change them often, and do not disclose them; and

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

5) Ascertain and understand the laws, policies, rules, procedures, contracts, and licenses applicable to their particular uses; and

6) Comply with all federal, state, and other applicable laws, all generally applicable university regulations, and all applicable contracts and licenses; and

7) Use only those university IT resources and information systems that they are authorized to use and use them only in the manner and to the extent authorized; and

8) Refrain from unauthorized attempts to circumvent the security mechanisms of any university IT resource or information system; and

9) Refrain from attempts to degrade system performance or capabilities or damage IT resources, information systems, software, or intellectual property of others; and

10) Use multi-factor authentication required for all administrative and functional access to IT resources that store, process, or transmit personally identifiable information.

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

4.3 User Prohibitions

4.3.1 Users shall not do the following:

1) Share passwords or accounts; or

2) Copy or change system files or software without authorization from a system administrator; or

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

4) Crash machines or systems recklessly or deliberately; or

5) Lock a public shared technology asset without authorization from a supervisor or asset manager; or

6) Use the university technology assets for disruptive or illegal activities; or

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

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

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).

4.4 System Administrator Rights and Responsibilities

4.4.1 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.

4.4.2 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

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

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.

4.6 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 IT resources and information systems. 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 IT resources and information systems they support.

4.6.3 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.

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

4.6.5 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.

4.7 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 doing the following:

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

2) Enabling the appropriate university personnel to make well informed decisions regarding risk and risk management; and

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

4) Providing a systematic methodology to assess and manage information security risk for the University; and

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.

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

1) Protect any IT resources and information systems under their management from compromise; and

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

3) Configure the IT resources and information systems to reduce vulnerabilities to an acceptable risk level; and

4) Install anti-virus or other anti-malware tools, install relevant security patches, and implement security best practices for IT resources; and

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

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 IT resources, information systems, technology assets, and 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 effective procedures for granting authorization, tools, and practices to authenticate authorized users.

4.8.2 The appropriate university system administration group shall issue university accounts after the request is authorized appropriately and documented adequately.

4.8.3 The appropriate university system administration group shall authenticate university accounts at a minimum via unique login and complex passwords.

4.8.4 The appropriate university system administration group shall 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.

4.8.5 The appropriate university security group shall conduct periodic reviews of authorized access commensurate with the assessed level of risk.

4.9 Change Management

4.9.1 Any changes to university production IT resources and information systems that store, process, transmit, or maintain confidential data shall be authorized, tested, documented, and approved prior to implementation. Digital Transformation will notify the affected entities.

4.10 Physical and Facility Security

4.10.1 University IT resources 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 institution shall maintain an inventory of all internal or third-party IT resources 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 IT 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.

4.12 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, IT resource, and information system access to networks and network services shall not compromise the security of the network services by ensuring the following:

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

2) Appropriate authentication mechanisms are applied for users, IT resources, and information systems.

4.13 Log Management and Monitoring

4.13.1 The appropriate IT personnel, in coordination with the ISO, shall configure university IT resources, information systems, and 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.

4.14 Information System Media Handling

4.14.1 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.

4.14.2 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 or 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 such media to authorized personnel.

4.14.6 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.

4.15 Future Technology Needs Assessment

4.15.1 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.

4.16 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 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 shall audit systems used for university business to ensure compliance with this policy and industry security standards.

4.18 Violations

4.18.1 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.

4.18.2 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.

4.19 Security Standards

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

4.19.2 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 IT assistance as needed.

4.20 Enforcement

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

4.21 Exceptions to Policy

4.21.1 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 Review and Maintenance of Policy

4.22.1 The IT Oversight Committee, 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:

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

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

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; and

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

5) Backups shall be moved offsite, and a fireproof vault shall be used if backups remain onsite. The offsite storage location shall be securely maintained and managed in a manner appropriate for the storage of university data; and

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

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 Owners of devices 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 Owners of devices 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 Owners of devices 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 Information Security Office (ISO). The incident must also be reported to the appropriate data steward and data custodian.

5.3 Private Sensitive Information (PSI) Incidents

5.3.1 If the compromised system contains Private Sensitive Information (PSI) as outlined in UVU Policy 445 *Institutional Data Management and Access*, IT personnel or the appropriate data owner must report the incident to the Office of General Counsel. Additional technical, forensic, and other support may be sought from outside the campus community.

5.3.2 If PSI has been accessed or compromised by unauthorized persons or organizations, IT personnel or the appropriate data owner must consult with their dean, department head, or supervisor; the ISO; 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.

5.4 Control Activities

5.4.1 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

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

POLICY HISTORY		
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