University of Phoenix®

University of Phoenix Policy
Information Security

Effective: 9/2/2025	**Supersedes:** Information Security V5, 9/17/2024
Policy Owner: Information Security	**Version Number:** 5.1

Table of Contents

University of Phoenix®

1.0 Overview

University of Phoenix (the “University” or “UOPX”) is committed to the security of our systems, assets, and information. The Information Data Security policy has been formed from industry standard security frameworks, ISO/IEC 27001 and NIST 800-171, as foundations for the University’s Information Security Program. The University’s Information Security policies, in conjunction with its comprehensive Information Security Standards, document the University’s Information Security Program, controls, and business requirements. These requirements apply to all technology, including platforms, information/data, information processing/computer systems, and networks (collectively known as “information assets”) owned by or entrusted to the University, including any sensitive, protected, or confidential institutional data accessed or maintained on a personal device. Just as technology and our industry changes, the Information Security Program, these policies, and Information Security Standards are also subject to change.

2.0 Scope

All employees, including associate, lead, and practicum faculty, contractors, consultants, temporary workers, business partners, and any other persons or entities doing business on behalf of the University.

3.0 Policy

3.1. Information Security Program Implementation, Oversight, and Enforcement

The Chief Information Security Officer (CISO)/VP is identified as the qualified individual responsible for the development, implementation, monitoring, and enforcement of the University’s Information Security Program and periodically provides updates on its status to the University’s IT governance bodies, Executive Leadership, and its Board. The Chief Information Officer is responsible for oversight and direction of the CISO/VP. In addition to your general responsibilities outlined in this policy, the Information Security Standards, and related University policies, the CISO/VP will be responsible for oversight of UOPX IT, and/or individuals or the teams that may be designated to perform other essential information security and cybersecurity risk management functions contributing to the Information Security Program’s implementation and compliance. For more information and to access the Information Security Standards listed here, please see the Resources on the Policy Library. The CISO/VP is responsible for oversight and governance of any 3rd party service provider that may assume oversight or implementation responsibilities for the security program. The CISO/VP will be responsible to report on the status of the security program including identified risks, control decisions, results of testing, security events, security violations, and University’s compliance to the Board of Directors or the equivalent Executive Leadership on an annual basis at a minimum.

The CISO/VP is identified as the qualified individual responsible for the oversight of connectivity of machines and servers to the University network that do not comply with this policy, or its associated Information Security Standards. Any systems that do not comply with standards may be limited or removed. Violations of this policy may result in corrective action up to and including suspension or revocation of accounts and access to networks, non-reappointment, dismissal or termination of employment, as well as referral to law enforcement, as appropriate. In addition, those found to have violated this policy may be held accountable for the financial penalties, legal fees, and other remediation costs associated with a resulting information security incident, data/security breach, and/or other regulatory non-compliance

3.2. Information Security Risk Assessment

A written cyber risk assessment will be periodically conducted (annually at a minimum) by the CISO/VP to identify internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure or compromise of such information. The CISO/VP will be responsible for establishing risk assessment criteria to evaluate and categorize identified information security risks, criteria for the confidentiality, integrity, and availability of your information.

The CISO/VP will be responsible for ongoing governance of identified risks including assignment of remediation or mitigation steps to resolve or appropriate risk acceptance and approval by the CISO/VP. The CISO/VP will periodically perform risk assessments (annually at a minimum) to re-assess previously identified information security risks and identify any additional risks that could result in the unauthorized disclosure or compromise of organizational or customer information.

The CISO/VP will be responsible to evaluate and amend the information security program based on risk assessments, results from testing and scanning activities, and any material changes to business operations or processes.

3.3. Safeguards to Control Identified Risks

The CISO/VP will develop and implement safeguards to control the risks identified in the risk assessments. Categories that will be developed and implemented include:

3.3.1. **Access Controls** - The University has established technology and physical controls to protect information and information systems from unauthorized access, modification, or disclosure. All authentication systems will be constructed in such a way as to effectively preclude unauthorized access. Password length, password complexity, password expiration, and password history, are used by authentication systems to mitigate the risk of unauthorized access. CISO/VP will periodically review both technology and physical access granted to users who access customer information.

Business authorization to information and information systems will be granted using the principle of least privilege by business need and in compliance with applicable local, state, federal, and international laws and regulations. Existing access and access control rules are periodically reviewed and approved by relevant data stakeholders. Access for critical applications must be reviewed at least quarterly including acknowledgment from the application Product Owner that those permissions are appropriate for each user, or permissions must be removed/modified. For non-critical applications, access reviews must be conducted based on the number of individuals with access, the number of individual changes, and the type of access. Non-critical application reviews must be performed at least annually.

University IT utilizes a formal review and approval process to manage the user access lifecycle and to designate appropriate assignment of user access rights, preventing unauthorized access to information systems, including management of privileged user accounts and access rights. University IT establishes individual accountability through provisioning processes that issue each person a single, unique username and user-defined password.

For network, device, and application access, University IT establishes appropriate interfaces and security mechanisms to protect and segregate the University network from those networks owned by other organizations and/or public networks. University IT prevents unauthorized access to information system devices by restricting access to authorized administrators only. Audit mechanisms monitor inappropriate use of privileged accounts. Authentication credentials must be encrypted when stored or transmitted, including over the internal network. University IT shuts down sessions after a defined period of inactivity.

For remote access, University IT enforces appropriate information security controls for remote access using Virtual Private Networks (VPN). Just as when working on premises, those authorized to work remotely may only access systems and resources that they have permission and rights to use. Connections provided for use by external parties will be made available only at the time of need and must be immediately deactivated after use

3.3.2. **Asset Management** - All University information systems, including the data processed, managed, or stored therein are considered assets belonging to the University. To the full extent allowed by

law, you should have no expectation of privacy when using University assets. This includes electronic communication systems (email, voice, and chat) as well as messages generated by these systems.

All employees, including associate and lead faculty, contractors, consultants, temporary workers, business partners, and any other persons or entities doing business on behalf of the University are responsible to protect University assets from theft, destruction, or misuse.

The University identifies all assets, and the asset inventory is maintained in a centralized index to include responsible data stakeholder(s), owner(s), and/or custodian(s). The University designates management of all information and assets associated with data centers.

3.3.3. **Acceptable Use** - The use of University assets should be in a professional, lawful, and ethical manner. The University assets must never be used for activities that have been identified as unacceptable in the Asset Management Responsibility and Acceptable Use policy, without express approval from Information Security.

Managers have the discretion to allow limited personal use of University assets if it does not violate this policy, the cost to the University is insignificant, and the use does not deplete the value of our assets, interfere with productivity, or create risk or liability for the University.

For more information about acceptable use and to review your responsibilities, please refer to the Asset Management Responsibility and Acceptable Use policy.

3.3.4. **Essential Business Process, System, Data & Location** - The University will identify and manage core functions and associated essential dependencies (including staff, facilities/location, data, systems) that align to each function's day-to-day purpose and objectives. The University will assess priority of each core function and its associated dependencies to identify risks, establish or maintain existing risk mitigation strategies or risk acceptances.

3.3.5. **Encryption of Customer Data** - The University will maintain security controls or mitigating risk controls to encrypt all customer information transmitted over external networks and at rest. Any exceptions or compensating controls will be reviewed and approved by the CISO/VP.

Data Classification: As a critical asset, information must be protected according to its nature, value, and sensitivity in support of our core business functions. We use a hierarchical data classification system:

- ***Public*** – For general public use, not sensitive in nature, such as directory information, which may be released under certain conditions.
- ***Confidential*** – For internal use in the course of University business, considered to be valuable and proprietary, not for release without authorization.
- ***Protected*** – For restricted internal use in the course of University business, considered private, regulated, and/or valuable, not for release without authorization.

Please reference the Data Classification, Definitions, and Retention standard for more information.

3.3.6. **Software Development & Product Ownership** - The University adheres to secure development practices for all internal and externally developed applications that access, transmit, and/or store customer information. The University maintains procedures to assess and test any externally developed application that accesses, transmits, and/or stores customer information. Product Owners designated for application systems are responsible for the security of the development environment and must review all proposed changes to confirm they do not compromise security controls.

3.3.7. **Multi-Factor Authentication (MFA)** - The University requires MFA implementation for all users accessing any University information system. MFA shall be implemented for all applications and data transfers external to the University network.

3.3.8. **Secure Disposal of Customer Information** - Records containing University information, including confidential, proprietary, or personal information of employees and consumers, must be disposed of in a manner that renders them inaccessible and unreadable. The University's approved method for disposal of paper materials is shredding through an approved, NAID certified secure shredding supplier. Likewise, electronic records and other media are disposed of by a means that ensures that confidential data cannot be reconstructed or recovered.

Disposal occurs only when the records or data have been retained longer than required by the University's Records Retention Schedule and are not subject to Preservation Hold. Department leaders are responsible for receiving approval from Ethics, Compliance, and Data Privacy (ECDP) in advance of disposal of any records or data. Disposal of records prior to scheduled disposition is prohibited. Please see the Records and Data Management Policy and the Records and Data Management and Legal Preservation sites for more information. The University will periodically review the Records and Data Management Policy and the Data Classification, Definitions, and Retention policies to mitigate retention of any unnecessary data.

3.3.9. **Media and Information Handling** - University IT implements controls to prevent unauthorized disclosure, modification, removal, or destruction of information assets and interruption to business activities.

- **Removable Media:**
  Appropriate encryption must be applied to data stored on removable media where business process requires such use. Removable media may not be connected to or used with any computer that is not owned or leased by the University without the explicit permission of Information Security. Regulated and Confidential information is stored on removable media only when required in the performance of assigned duties or when providing information required by other state or federal agencies. When Regulated or Confidential information is stored on removable media, it must be encrypted in accordance with the University's Cryptography Standard.
- **Exchange of Information:**
  The University determines when information assets can be shared with others after thorough consideration of our legal and contractual obligations, business needs, and the best interests of our consumers. When we do exchange information with an external organization, University IT implements controls to maintain the security of that information and software. Exchanges of information and software are governed by formal exchange agreements which include non-disclosure clauses, as appropriate. Unless expressly stated otherwise in exchange agreements, University IT applies equivalent levels of data protection for both University and non–University data.

  You may not share information assets with any outside entity without 1) a written agreement in place that protects the information being exchanged, 2) an evaluation of the entity's information security processes, and 3) documented procedures that are consistent with the safeguards set forth in this policy, or as otherwise required by applicable law.
- **Electronic Commerce Services:**
  University IT secures our electronic commerce services and monitors the integrity of their use, particularly the publicly available systems. All international and domestic Internet domain names must be approved by the CIO or CMO, or their designees, including all existing domain names involved in mergers and acquisitions.

3.3.10. **Change Management** - University IT maintains the security of application system software and information by strictly controlling changes to non-production and production environments. When operating systems are changed, business critical applications are reviewed and tested as

appropriate to ensure there are no adverse effects. Teams must collaborate with University IT to ensure test data is selected carefully, protected, and controlled. Production data must never be used in non-production segments, systems or applications. PI data will be removed and anonymized, and any controls or regulatory and privacy expectations are extended to the test data and the environments in which it resides. University IT evaluates, assesses, and tests security during outsourced software development to ensure it meets the same information security controls governing the internal development of applications.

3.3.11. **Access and Log Monitoring** - System monitoring is used to check the effectiveness of information security controls and to verify compliance with the Information Security Program. University IT is responsible for logging and monitoring the activity of authorized users accessing information systems to perform business activities as well as detecting unauthorized activities and relevant information security events. Audit logs must be formatted, stored, and protected to ensure integrity and to support enterprise-level analysis and reporting. To facilitate analysis and reporting, all system clocks must be synchronized with an agreed accurate time source. Audit logs must record all relevant activities, exceptions, and information security events initiated by all users and administrators. Audit logs must be kept for an agreed period as prescribed in the Records and Data Management and Data Classification, Definitions, and Retention policy.

3.4. Network Monitoring, Controls & Testing

University IT is responsible for ensuring the regular testing and/or monitoring of the controls, systems, and procedures that detect and prevent attacks on information systems. Based on relevant security risks, the University will maintain continuous monitoring, penetration testing on an annual basis, and vulnerability assessments including systemic scans or reviews of information systems every six months or upon material changes to business operations via a managed 3rd party service or internal resources.

University IT is responsible for the secure design, operation, and management of network devices. University IT has sole authority to acquire network equipment and to build and maintain the University network infrastructure, except where University IT has delegated specific authority outside of IT. All systems and equipment connected to the University network must be approved by IT, including but not limited to firewalls, switches, routers, and wireless devices. Devices that do not meet the University configuration standards will not be used on the University network unless authorized through an approved policy exception.

University IT implements appropriate controls such as strong cryptography and security protocols to protect information traversing public or other untrusted networks. Access to network devices is limited to authenticated accounts that have been explicitly assigned for administrative responsibilities. Administrative accounts for all network components will be validated as appropriate no less than once each quarter. Stateful packet inspection must be used to control access between network zones, and any network traffic that is not explicitly permitted must be denied access. Direct access from endpoint devices to data center network segments is only permitted by approved exceptions from the VP, Information Security and a VP responsible for risk acceptance of the risk associated with the request. Approved exceptions must only be conducted through approved secure access techniques.

University IT is responsible for management of relevant technical vulnerabilities within information systems including providing timely awareness, evaluation of the University's exposure, and mitigation of the associated risk.

Product owners and system administrators must implement controls to prevent, detect, contain, and correct threats to the security of the University's information systems and its data from fraudulent activities or unintentional errors. Information security controls are to be documented, maintained, communicated, and made readily available for procedural operations.

University IT verifies the correct and secure operation of all networks and information systems, including the development of appropriate operational procedures and segregation of duties, to reduce the risk of

negligent or deliberate system misuse. To reduce the risk of unauthorized access or changes to operational systems, University IT logically separates production networks from non-production networks, periodically reviews access controls to confirm appropriate levels, and verifies change control procedures are followed.

CISO/VP will be responsible for continued evaluation of information security risks. CISO/VP will adjust and update the security program based on any risks identified in the vulnerability scanning and annual penetration testing or any other identified material change to University operations or processes.

3.5. Information Systems Acquisition, Development, and Maintenance

Information Security and Enterprise Architecture are an integral part of the University's operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. University IT manages and controls any additions to or modifications of these systems. Information security requirements are documented throughout the process. The University development process includes requirements for authenticity and message integrity in applications. Prior to any new or enhanced development, Product and Platform teams must collaborate with University IT and follow the documented templates and guides which require documentation of security controls as part of the requirements definition.

No modifications may be made to commercial software packages that would invalidate continued vendor support of the software. All commercial software must be covered by current vendor support agreements.

- **Correct Processing in Applications**
  The University manages errors, loss, unauthorized modification, or misuse of information in applications, including those developed in-house, by implementing appropriate application controls such as validation of input data, internal processing, and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable, or critical information and will be determined based on security requirements and risk assessment
- **Cryptographic Controls**
  University IT protects information using cryptographic controls and key management for sensitive information at-rest or in-transit, when required by laws/regulations or when deemed otherwise appropriate.
- **Security of System Files**
  University IT controls the generation of, and access to, system files and program source code. Procedures are also in place to control the installation of unauthorized software on operational systems

3.6. Protection Against Malicious Activity and Mobile Code

To protect the integrity of software and information assets, University IT utilizes automated controls to help prevent, detect, and remove malicious code and to control mobile code (local execution of untrusted code) within the computing environment. Additionally, awareness programs are provided to inform users of the dangers of malicious code and how to minimize risks associated with malicious code. Application Support Teams are responsible for ensuring patches are applied in a timely fashion and for ensuring the design and development of their applications follows secure coding principles and standards. Please review the Secure Code Practices standard for more information.

University systems and software must maintain appropriate levels of security updates (patches) to reduce risk to the University and meet regulatory requirements. Security updates are applied using a methodology that focuses first on high-impact systems and high-risk vulnerabilities. Unless otherwise mandated by regulatory requirements, University security updates maintain the following patch levels:

- **High-risk** systems have high-risk vulnerabilities patched in 60 days or less. Risk determination is the responsibility of Information Security. Risk, as determined by the

authoring patch companies, may not necessarily represent the University's determination of risk.

Additionally, where security patch application cannot be easily automated and manual application represents significant organizational effort, the 60-day requirement can be adjusted to better align with organizational capabilities. Regardless of circumstances, all high-risk patches should be applied no less frequently than 90 days from patch availability.

- **Moderate risk** systems have high-risk vulnerabilities patched in 90 days or less.
- All other systems should have all vulnerabilities patched in 120 days or less.
- Vulnerability assessment and patching will only be performed by designated individuals.
- All patches must be acquired from relevant and authorized vendors and/or other trusted resources. Each patch must be authenticated, and the integrity of the patch verified.
- New servers (e.g., virtual and physical) and software must be fully patched before coming online to limit the introduction of risk.
- All patches must be tested before being deployed in production.
- Where the use of mobile code is authorized, configurations ensure that the authorized mobile code operates according to a clearly defined security standard and prevent the execution of unauthorized mobile code when possible.

3.7. Back-Up Standard

To maintain the integrity and availability of information and information systems, University IT establishes a back-up standard and strategy which aligns with the Disaster Recovery Program and Records and Data Management policy. University IT is also responsible for taking and testing back-up copies of information and software regularly following that back-up standard. As servers in cloud environments that do not contain application data (frequently referred to as "stateless" cloud servers or "full stack deployment" servers) are never used for recovery purposes and are regenerated from a standard image, they do not need to be included in the back-up program.

3.8. Security Awareness Program

The University maintains policies and procedures that govern security awareness program objectives, delivery methods and cadence which is documented in the University Policy for the Security Awareness Program. Information Security, CISO/VP and/or other University departments will send frequent reminders of this and/or other related policies to remind you of your responsibilities, update you on important changes based on risks identified in internal risk assessments, and assist you in complying with your obligations as it relates to information security. The University offers and, in some cases, requires your completion of awareness training or acknowledgement that you follow these established policies and procedures. Information security staff will receive sufficient training and maintain sufficient security knowledge to address existing security risks and understand potential security threats and appropriate responses.

3.9. Supplier Risk Management

The University relies on third-party suppliers and service providers to provide certain products and services. Prior to supplier onboarding, suppliers require a due diligence assessment to determine risk. Products and services with an information technology or data component may require additional review prior to contracting or purchasing. During this Supplier Due Diligence process, risks to the University information and assets will be assessed, and additional controls may be required in accordance with this policy and the Supplier Risk Management policy.

All agreements with external entities which involve accessing, processing, communicating, or managing University information, information entrusted to the University, or University-owned or managed

information systems must include all relevant security requirements as documented in this Information Security policy and the Third-Party Information Security Standards.

University IT implements and maintains an appropriate level of information security and delivery when engaging third-party service providers. University IT validates the implementation of agreements, monitors compliance with the agreements, and manages changes to meet all requirements agreed to with the third party. University IT also regularly monitors, reviews, and audits the services, reports, and records provided by third-party providers.

3.10. Incident Response

The University has a comprehensive Incident Response Plan (IRP) that documents the purpose, objectives, and scope of how the organization responds and recovers from an incident that materially impacts the confidentiality, integrity, or availability of customer information. The plan dictates the roles and responsibilities of Incident Response participants including decision making topics such as who can declare an incident, when an incident should be declared, and who to include in the response. The IRP documents the process and responsible owners for external and internal communications during an incident. Information Security applies a consistent and effective approach to the management of information security incidents including internal processes for responding to an event. Information Security is responsible for managing incident response and developing incident response procedures so that information security incidents and concerns associated with information systems are communicated in a manner allowing timely corrective action to be taken. Logs and other evidence are collected and retained following compliance and legal requirements including documentation and reporting regarding security events and related incident response activities. Any identified weakness related to information systems will be remediated with appropriate updates and revisions to the IRP.

All Incident Response Team members are required to report any concerns relating to a flaw, or bypass of Information Security policies or standards, or any confirmed or suspected information security incident(s), to infosec@phoenix.edu.

Where legal action (either civil or criminal) against an individual or organization occurs following an information security incident, University IT will make available, collect, retain, and present evidence as needed to conform to the rules in the relevant jurisdiction(s). UOPX legal counsel will be responsible for all required breach notifications to federal regulators and/or agencies as referenced in the UOPX IRP.

For additional guidance please refer to the Incident Response Plan.

3.11. Human Resources

Prior to employment, managers are responsible for including information security responsibilities in job postings and defining security roles and responsibilities for University positions as well as monitoring these requirements during an individual's transition to employment. During pre-employment, background checks on all candidates for employment, contractors, and third-party users are carried out following relevant laws and regulations, and as appropriate and proportionate to the business requirements, classification of the information to be accessed, and perceived risks.

The University requires that individuals agree to the terms and conditions of their employment or contract such as by acknowledging their receipt of and their responsibilities under this policy.

Regarding staff termination or change of employment, University leadership defines and assigns responsibilities for performing employment termination or change of employment such that physical information assets are recovered and all access to information systems are promptly adjusted or revoked. University leaders must confirm all University assets are returned upon an individual's termination of employment, contract, or agreement and that access rights to information and information processing facilities are likewise removed or adjusted upon change.

3.12. Physical and Environmental Security

- **Secure Areas:**
  University locations that house network equipment or information systems ("network or server closet") are protected from unlawful and unauthorized physical intrusion/access, theft, fire, flood, and other hazards. The University maintains physical security perimeters (such as walls, card-controlled entry gates, and/or reception desks) to protect authorized information processing facilities, and only authorized personnel are allowed access. The University works with co-location providers to implement appropriate physical security measures to protect University assets.
- **Equipment Security:**
  University IT protects all essential data center systems, co-location facilities, and equipment from power failures and other disruptions that may be caused by failures in supporting utilities. All systems assigned to individual users (desktop, laptop, tablets) and peripherals (storage media) adhere to documented protection standards and other required security controls. Comparable physical security controls are also applied to off-site equipment. University IT confirms that all equipment containing storage media is inspected so that any sensitive data and licensed software has been removed or securely overwritten prior-to disposal. Equipment, information, or software should never remove off-site without prior approval.

3.13. Compliance

The University ensures compliance of information systems through ongoing control owner attestation and by regularly auditing for compliance with information security policies, standards, and documented controls. The University likewise establishes information security controls to safeguard the integrity and prevent misuse of audit tools used for information security audits. The University ensures that audit requirements and activities involving checks on operational systems are planned and scheduled to minimize the risk of disruptions to the business.

4.0 Policy Exceptions

Certain situations or emergencies may occur when practical considerations or modifications to this policy are necessary, such as the introduction of new legal or regulatory obligations and situations where application of the policy standards pose certain system security challenges and/or tradeoffs. If you believe a situation warrants a policy exception, raise the issue with your manager or leader. Management, in conjunction with Information Security, ECDP, relevant Information Asset Owner/s, and other stakeholders will make a risk-based decision to permit or deny policy exceptions.

All policy exceptions require the approval of the CISO/VP of Information Security. The CISO/VP of Information Security is responsible for recording exceptions to this policy and for following-up with the Information Asset Owners at least annually to assess progress towards resolving the issue that resulted in the need for an exception. In an emergency where prior notification and acceptance is not possible, exceptions must be reported to the CISO/VP of Information Security within 24-48 hours for retrospective review and approval.

5.0 Related Policies and Procedures

Asset Management Responsibility and Acceptable Use Policy
Information Security Standards
Data Management and Retention
Data Classification, Definitions, and Retention Metadata Policy
Supplier Risk Management Policy
Secure Code Practices Standards