Information Security Policy

August 28, 2020
Version 2.2

TABLE OF CONTENTS

1 Scope

1.1 Introduction and objectives

1.1.1 This Information Security Policy consists of a comprehensive set of principles, policy statements and references to relevant information security standards. Collectively, these will serve as the authoritative source for the full range of information security controls required by the University of Phoenix. Its objective is to communicate management directives and standards of care to ensure consistent and appropriate protection of information and information systems in use across the University.

1.2 Purpose

1.2.1 The purpose of the Information Security Policy is to provide management direction and support for information security in accordance with UOPX business requirements, and relevant laws and regulations.

1.3 Status and applicability

1.3.1 This Information Security Policy has been reviewed and approved by the Chief Information Officer, IT managers and the VP, Information Security. Additionally, this Information Security Policy has been accepted by the Data Privacy Office in coordination with the Data Governance Council. With this approval, UOPX confirms that this policy is directly aligned with business objectives. Additionally, the continued periodic review and approval of this policy demonstrates managements support for, and commitment to, information security across the organization.

1.3.2 This Information Security Policy is reviewed at least annually or if significant changes occur, ensuring continued suitability, adequacy, and effectiveness. The Ethics, Compliance and Data Privacy office will have oversite on reviews in coordination with Internal Audit.

1.3.3 It is applicable:

- Throughout UOPX including all UOPX locations
- To all UOPX employees and others working on behalf of UOPX in a similar capacity including contractors, consultants, temporary Workers, student placements etc. (known collectively throughout as “Workers”)
- To all information / data, information processing / computer systems and networks (collectively known as “information assets”) owned by UOPX, or those entrusted to UOPX by third parties.

1.3.4 It is NOT applicable to students.

1.3.5 It supersedes previous versions of the Information Technology Personnel Information Security Policy as well as the Information Security Policy resident in the University of Phoenix Employee Handbook.

1.3.6 These policy statements are supported by a range of security controls documented within operating documents and other controls socialized with Workers from time to time by management through information security procedures and guidelines. The supporting controls refer to, and gain authority from, the information security policy statements included in this manual.

1.4 Intended audience

1.4.1 This policy manual is primarily intended for use by:

- **Workers** comprising all UOPX employees (including temporary employees) and third parties (such as consultants, contractors, support/maintenance staff) acting in a similar capacity. Workers are broadly informed of the UOPX information security policies through this manual and are specifically informed of any standards and procedures that are directly relevant to their activities through the associated security awareness activities, terms and conditions of employment, management briefings etc.

1.5 Policy exceptions

1.5.1 Despite the care that has been taken in authoring, reviewing and approving this policy manual, the authors cannot possibly foresee all possible circumstances or situations in which it might apply. It is therefore conceivable that exceptional situations or emergencies may occur when practical considerations clearly override or negate the policy statements made herein. Examples include the introduction of new legal or regulatory obligations that conflict with specific policy statements or in unique situations where following the policies to the letter would cause unacceptable health and safety risks.

1.5.2 Under normal circumstances where an individual believes that a situation warrants a policy exception, it is their responsibility to raise the matter with management. Management, in conjunction with the Information Security team, relevant Information Asset Owner/s and other stakeholders, will take an explicit risk-based decision on whether to permit or deny policy exceptions.

1.5.3 Where a policy exception is permitted, the approval of a VP level or above in the affected area of business will be required. The VP will assume personal accountability for any security incidents that arise as a direct result of the exception. If, for example, a given IT system cannot be configured to enforce password length and complexity rules stated in section 9.3.3, the corresponding Information Asset Owner may request a policy exception but will be held to account for any security incidents arising from user authentication failures or incidents as a result of the policy exception.

1.5.4 The VP, Information Security is responsible for recording exceptions in the exceptions database, and for following-up with the Information Asset Owners at least once a year to assess progress towards resolving the issue that resulted in the need for an exception.

1.5.5 The UOPX Information Security Policy, along with supporting Standards, is in place to assist UOPX in complying with legislative and regulatory requirements. Compliance is a task for everyone, including every Worker. In certain specific circumstances it may not be feasible to comply with a policy or standards requirement. In such cases, it is critical to document each instance of non-compliance by filing an exception with the owner of the policy or standard and receiving an approved waiver.

1.5.6 **Emergency policy exceptions:** Where justified and necessary under exceptional circumstances, limited policy exceptions may be made without prior VP approval. Where prior notification and acceptance of policy exceptions is not possible (for example in an emergency), exceptions must be reported to Information Security as soon as possible thereafter (within 24-48 hours) for retrospective processing under the policy exceptions process noted above.

1.5.7 Deliberate non-compliance with one or more information security policies that has not been notified to and agreed by the VP, Information Security may be treated as a disciplinary matter and result in actions up to and including termination.

1.5.8 By definition, emergency exceptions are not anticipated to be routine in nature. Where the need for policy exceptions arise under routine circumstances in the normal course of business, the routine policy exceptions process noted in section 1.5.2 must be followed.

1.5.9 Emergency policy exceptions must meet any of the following criteria:

- There is significant chance of health and safety issues if the exception is not implemented in a timely manner.
- There is an outage that is preventing active students from attending class, or otherwise progressing in their program.
- The issue is preventing future students from applying, enrolling or interacting with a UOPX Worker that could assist in the application or enrollment process; and
- The issue is materially and/or persistently disrupting Workers from providing necessary support to students and/or potential students.

1.6.4 Document change control

1.6.4.1 Since it incorporates formal statements of UOPX policy, this manual is subject to a strict change control process. Workers will be notified of changes as appropriate.

1.6.4.2 Feedback comments, corrections and improvement suggestions on this policy manual (including any areas that are not sufficiently well covered) are welcome from any part of UOPX at any time. technology-informationsecurity@phoenix.edu.

1.6.4.3 Proposed alterations to the manual will be analyzed and developed by Information Security in conjunction with relevant subject matter experts (SME). Updates may be circulated for comment, clearly labeled as DRAFTs. DRAFTs are not intended for implementation and do not necessarily reflect official UOPX policy until they are formally approved and posted by Ethics, Compliance and Data Privacy and the Data Governance Council.

1.6.4.4 The manual will be annually reviewed by the VP Information Security and additional SMEs as necessary. The Data Privacy Office, Data Governance Council and the CIO will approve changes.

2 Terms and Definitions

Access control - Security control designed to permit authorized access to an information system.

Administrative network - UOPX network that houses internal applications.

Administrative areas - Physical space that is for Worker use only (not for students and/or faculty members). Administrative areas are not considered public and will be physically secured from the public areas through key or cipher locks or badge access system.

Audit log - Record showing who has accessed a system and what operations were performed in a time period.

Authentication - Process where users or information sources prove they are who they claim to be, or verification of data stored, transmitted or exposed to unauthorized modification.

Backup - A secondary copy of data on a separate form of media, e.g., tape media, remote disk storage system, cloud storage, CD-ROM, DVD, etc.

CVV, CVV2 or CVC2 data – Various credit card security codes used for 'card not present' transactions.

Cloud Computing – The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Credit Card information – Cardholder Name, credit card number, expiration date, and CVV.

Company asset - Any product or service produced or provided by UOPX and/or any of its subsidiaries.

Corporate approver - Assigned advertising entity at the corporate level of the Company subsidiaries, also known as the "approved creative".

Cryptographic Controls - These are the policies, procedures, and standards around the setup, implementation, and maintenance of encryption technologies and their encryption keys.

Data centers - Centralized locations as designated by UOPX IT (designed to store and secure computer information systems equipment) hosted by third-party providers.

Degaussing - Method to magnetically erase data from magnetic tape.

Electronic communications systems - Media to transfer information electronically, including Internet, voice mail, electronic mail and fax.

Electronic marketing - Any marketing strategy that targets prospective students or other potential stakeholders through an electronic communication channel, typically via e-mail or Website advertising.

Encryption Technologies - The use of ciphers and algorithms to protect data from unauthorized access. This usually uses some form of Key to unlock/lock the data in an encrypted pattern.

Encryption key - Unique, secret data block used to encrypt data.

Environment - When used with the words "development", "test" or "production", indicates a separate instance of source code and data for a particular purpose.

Information system - System consisting of the network of all communication channels used within an organization including operating systems, infrastructure, business applications, services, etc.

FERPA - Family Educational Rights and Privacy Act.

Information Asset Owner – A person responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure the information assets are properly protected and that their value to the organization is fully exploited.

Information Asset – A body of knowledge that is organized and managed as a single entity.

Internet - External sites available to personnel who have a network connection.

IP address - An Internet Protocol address that is assigned to devices participating in a computer network.

IRN – Individual Record Number assigned to UOPX Students.

Mass communication - Any marketing campaign using e-mail or mail where the recipients are leads that belong to multiple individuals.

Media - Various devices on which data is stored—USB Drive, tape, hard disk, CDROM, etc.

MP3 - MPEG-1 Audio Layer 3, a de facto standard of digital audio compression for the transfer and playback of music on digital audio players.

NDA - Non-disclosure agreement.

Non-work time - Off-duty hours, such as lunch periods, time before or after a workday, weekends or holidays.

Password cracking - Using software to guess at a password or try to re-create a password using a dictionary of predefined words.

PI (personal information) – information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

PII – Personally Identifiable Information; any data that could potentially be used to identify a particular person (e.g. full name, social security number, driver's license number, bank account number, passport number, etc.).

PIN – Personal Identification Number.

PST - Personal storage table used for email.

PVV - PIN Verification Value.

Remote access - Method and process of achieving access to the Company internal network from a remote external network using Virtual Private Network (VPN).

Risk – A situation involving personal or business exposure to danger, harm or loss.

Risk Management – The forecasting and evaluation of risks together with the identification of procedures to avoid or minimize their impact.

Security groups – Groups associated to cloud computing that provide security at the protocol and port access level. Working much the same way as a firewall, a security groups contains a set of rules that filter traffic coming into and out an instance.

Universal Serial Bus (USB) - External peripheral interface standard used to store information.

Virtual Private Network (VPN) - Use of encryption to provide a secure connection through an otherwise insecure network, typically the Internets.

Workers – Inclusive term used to describe Workers, Faculty, temporary Workers, custodians, contractors and others who utilize UOPX information systems.

3 Information Security Risk Management

3.1 Purpose

3.1.1 The purpose of the information security risk management policy is to provide practical guidance necessary for assessing and mitigating security risks to information and information systems within UOPX.

3.1.2 Information security risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Security risk management is the process of identifying security risks, assessing security risks, and taking steps to reduce security risks to a mutually agreeable acceptance level.

3.2 Assessing Information Security Risks

3.2.1 Information Security is responsible for providing UOPX with an ongoing and systematic view of security risks to information and information systems, information projects and information strategy across UOPX at least annually.

3.2.2 UOPX uses Information Security Risk assessments to better understand and manage IT related risks to business systems, technology projects and business strategies.

3.2.3 Comprehensive and high-quality Information Security Risk Assessment enables the UOPX managers to make well-informed risk management decisions.

3.3 Addressing Information Security Risks

3.3.1 All information security risks identified during assessment will be tracked, prioritized and an action plan developed, approved, and executed. The response plans may include a variety of treatment options including retaining, avoiding, transferring, or reducing information security risks to acceptable levels through the introduction of additional security controls.

3.3.2 Recommended action plans will include an estimate of additional capital and operational costs.

3.4 Supplier Risk Management

3.4.1 The University of Phoenix relies on partners and service providers to provide quality services to Workers and students. At times, data is required for services that are contracted. During the supplier onboarding process, an evaluation must occur to determine appropriate risk levels depending on the type of data, classification and services being provided. The Supplier Risk Management policy defines details related to reoccurrence and process for appropriate evaluation of risk for each vendor.

4 Organization of Information Security

4.1 Purpose

4.1.1 The primary purpose of the information security organization is to establish a mechanism to manage information security across UOPX and beyond to external parties and that UOPX Management commit their support and provide overall direction.

4.2 Internal Organization

4.2.1 Information Security at UOPX is developed and defined by Information Security management, who coordinates information security responsibilities across many functional teams. UOPX Management will ensure organizational excellence and transparency using mutually agreed to performance metrics.

4.2.2 UOPX management will actively support information security through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

4.2.3 UOPX requires management authorization for implementation of data centers or placement of information processing systems outside of existing authorized data centers.

4.2.4 The UOPX approach to managing information security and its implementation (i.e. control objectives, policies, standards, processes, and procedures for information security) are reviewed independently at the direction of the UOPX Executive Leadership team.

4.2.5 UOPX management will ensure that appropriate contacts are established and maintained with information security authorities, special interest groups, security forums and professional associations.

4.3 External Parties

4.3.1 The Information Security program, policies and standards extend beyond the physical boundaries and Workers of UOPX. In all situations involving external entities, Information Security controls must be consistently and continually managed and assessed as compliant with the Information Security program.

4.3.2 Risks to UOPX information and information systems relative to external service providers will be assessed, and appropriate controls implemented before engaging with any third-party.

4.3.3 All agreements with external entities which involve accessing, processing, communicating or managing UOPX information, Information entrusted to UOPX, or UOPX owned or managed information systems will include all relevant security requirements as documented in this Information Security Policy and associated 3rd Party Security Standards.

5 Asset Management

5.1 Purpose

5.1.1 All information systems and all data processed, managed or stored by UOPX information systems are considered assets belonging to the UOPX. This includes electronic communication systems (email, voice and chat) as well as messages generated by these systems. The purpose of the information system asset management policy is to achieve and maintain appropriate protection of these organizational assets (hereinafter simply referred to as “Assets”).

5.1.2 To the full extent allowed by law, there must be no expectation of privacy with respect to the use of UOPX Assets**.**

5.1.3 An Asset is defined here as any information technology product or service produced or provided by the UOPX. Assets and resources include, but are not limited to:

- Information (data, databases, computer files, documentation, manuals, plans, audit logs, etc.)
- Software (application and system)
- Physical equipment (computer hardware, peripheral devices, network infrastructure and communication systems, monitors, projectors, displays and media)
- Services (email, chat, internet access)
-

5.1.4 This policy establishes direction for the acceptable use of UOPX Assets. Unacceptable use of UOPX Assets can lead to waste, fraud and/or abuse. For additional direction, please refer to the Personal Responsibility section of the Code of Ethics.

5.2 Responsibility for assets

5.2.1 It is the responsibility of every Worker to protect UOPX assets from theft, destruction, or misuse.

5.2.2 UOPX must maintain a comprehensive inventory of assets in a centralized index which is to include responsible data steward(s) ~~owner(s)~~ and/or custodian(s) of the asset.

5.2.3 UOPX must ensure that all assets are clearly identified and that the inventory of assets is current and actively maintained.

5.2.4 UOPX must ensure that all information and assets associated with data centers are ‘managed’ by a designated part of the organization.

5.3 Acceptable use of assets

5.3.1 UOPX assets are to be used in a professional, lawful and ethical manner. It is against UOPX policy to install or run commercial software without a valid license.

5.3.2 UOPX has identified documented and implemented rules for the acceptable use of UOPX Assets. UOPX Assets must not be used for activities which have been identified as unacceptable conduct by the UOPX.

5.3.3 Managers have discretion to allow limited personal use of physical assets if it does not reduce

productivity or interfere with job duties.

For additional information please refer to the Acceptable Use Standard. Link

5.4 Information Classification

5.4.1 UOPX recognizes information as a critical Asset that must be protected according to its nature, value, and sensitivity in support of the core business functions of UOPX. In addition, it is the policy of UOPX to protect information Assets according to documented UOPX standards. Information Assets are only made available to authorized entities on a risk-assessed, need-to-know basis, in compliance with policies, standards, and applicable local, state, federal, and international laws and regulations.

5.4.2 UOPX reserves the right to determine when information Assets can be shared with others to ensure sharing is not legally or contractually prohibited, and it is in the best interest of UOPX. This policy applies to data in all formats or media.

5.4.3 UOPX uses a hierarchical data classification system with four levels. Regulated represents the highest value and requires the greatest degree of internal controls and safeguards. Confidential information also represents high value and requires a significant degree of internal controls and safeguards. Internal Use Only is the mid-range classification and generally applies to inter-Company information. Public is the lowest classification and requires the lowest degree of internal controls and safeguards.

5.4.4 UOPX has established an appropriate set of controls for information protection, labeling and handling in accordance with the documented classification standard. (See 9.7 Media / Information Handling)

For additional information please refer to Data Classification Standards. Link

6 Human Resources Security

6.1 Purpose

6.1.1 The purpose of the Human Resources Security Policy is to identify the information security requirements for personnel that have an employment relationship with UOPX.

6.1.2 Management and personnel have different security responsibilities that apply prior, during, and at the time of termination of employment. Prior to employment, emphasis is on the awareness of the expected roles and responsibilities, the screening of prospects and the existence of agreements. During employment, policies establish responsibilities, education, training and linkage to detailed standards and processes used to address risk to information security assets. This policy also establishes rules to ensure a secure transition when employment has ended or has changed.

6.2 Prior to employment

6.2.1 Information security responsibilities must be considered during pre-employment background checks, included in job postings and monitored by management during an individual's transition to employment.

6.2.2 UOPX will ensure that security roles and responsibilities of Workers are defined and documented in accordance with the UOPX information security policy.

6.2.3 UOPX will ensure that background verification checks on all candidates for employment, contractors, and third-party users are carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

6.2.4 UOPX will ensure that as part of their contractual obligation, contractors and third-party users agree and sign the terms and conditions of their employment contract, which will state theirs and the UOPX responsibilities for information security.

6.3 During employment

6.3.1 Workers must be made aware of and are required to comply with their obligations under these information security policies plus the associated standards, procedures, guidelines, laws and regulations.

6.3.2 UOPX will ensure that management requires Workers to apply security in accordance with established policies and procedures of the organization.

6.3.3 UOPX will ensure that all Workers (where relevant) of UOPX receive appropriate awareness training and regular updates in information security policies and procedures, as relevant for their job function.

6.3.4 UOPX will ensure that there is a formal disciplinary process for Workers who have committed a security breach.

6.4 Termination or change of employment

6.4.1 A Worker's exit from or change of status within UOPX must be properly managed and controlled such that physical information assets are recovered and all access to information systems are promptly adjusted or revoked.

6.4.2 UOPX will ensure that responsibilities for performing employment termination or change of employment is clearly defined and assigned.

6.4.3 UOPX will ensure that all Workers return all UOPX assets in their possession upon termination of employment, contract or agreement.

6.4.4 UOPX will ensure that access rights of all Workers to information and information processing facilities are removed upon termination of employment, contract or agreement, or adjusted upon change.

7 Physical and Environmental Security

7.1 Purpose

7.1.1 The purpose of the physical and environmental security policy is to prevent unauthorized physical access, damage, or interference to UOPX offices, assets and business functions.

7.2 Secure areas

7.2.1 UOPX locations which house information systems (data centers) must be protected from physical intrusion, theft, fire, flood and other hazards. Data Centers must be safeguarded against unlawful and unauthorized physical access.

7.2.2 UOPX will establish and maintain physical security perimeters (such as walls, card-controlled entry gates or manned reception desks) to protect data centers and other authorized information processing facilities.

7.2.3 UOPX will establish and maintain appropriate entry controls to ensure that only authorized personnel are allowed access to data centers and other authorized information processing facilities.

7.2.4 UOPX will work with co-location providers to ensure appropriate physical security measures are implemented to protect UOPX assets.

7.3 Equipment security

7.3.1 UOPX IT will ensure that all essential data center systems, co-location facilities and equipment is protected from power failures and other disruptions caused by failures in supporting utilities.

7.3.2 UOPX will ensure that all Worker assigned systems (desktop, laptop, tablets) and peripherals (storage media) adhere to documented protection standards and other required security controls.

7.3.3 UOPX will ensure that comparable physical security controls are also applied to off-site equipment.

7.3.4 UOPX IT will ensure that all equipment containing storage media is checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

7.3.5 UOPX will ensure that equipment, information or software is not taken off-site without prior authorization.

8 Communication and Operations Management

8.1 Purpose

8.1.1 The purpose of the communication and operations management policy is to ensure correct and secure management of UOPX information systems and networks. System owners and system administrators must implement controls to prevent, detect, contain, and correct violations to ensure the security of data and the protection of UOPX information systems and networks from fraudulent activities or unintentional error.

8.2 Operational procedures and responsibilities

8.2.1 UOPX IT will ensure the correct and secure operation of all networks and information systems. This includes the development of appropriate operational procedures and segregation of duties, to reduce the risk of negligent or deliberate system misuse.

8.2.2 Information security controls are to be included in operational procedures as appropriate. Operational procedures are to be documented, maintained, and made available to all Workers who need them.

8.2.3 To reduce the risk of unauthorized access or changes to operational systems, UOPX IT will ensure that production networks are logically separated from non-production networks, and that proper access controls and adequate change control procedures are strictly adhered to and periodically reviewed.

8.3 Third-party service delivery management

8.3.1 UOPX IT will implement and maintain an appropriate level of information security and delivery when third-party service providers are engaged by UOPX. UOPX IT will periodically validate the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the information security services delivered meet all requirements agreed to with the third-party.

8.3.2 UOPX IT will ensure that services, reports and records provided by third-party providers are regularly monitored, reviewed, and audited.

8.4 Protection against malicious and mobile code

8.4.1 To protect the integrity of software and information assets, UOPX IT will utilize automated controls to 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.

8.4.2 UOPX systems and software must maintain appropriate levels of security updates (patches) in order to reduce risk to UOPX, and to meet regulatory requirements. Security updates should be applied using a methodology that focuses first on high impact systems and high-risk vulnerabilities.

8.4.3 Unless otherwise mandated by regulatory requirements, UOPX security updates should maintain the following patch levels:

8.4.4 High risk systems should have high risk vulnerabilities patched in 30 days or less. Risk determination is ultimately the responsibility of functional support teams. Risk as determined by the authoring patch companies may not represent risk as determined by UOPX. Additionally, where security patch application cannot be easily automated and manual application represents significant organizational effort, the 30-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.

8.4.5 Moderate risk systems should have high risk vulnerabilities patched in 60 days or less.

8.4.6 All other systems should have all vulnerabilities patched in 90 days or less.

8.4.7 Vulnerability assessment and patching will only be performed by designated individuals.

8.4.8 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.

8.4.9 New servers (e.g. virtual and physical) and software must be fully patched before coming online in order to limit introduction of risk.

8.4.10 All patches must be tested before being deployed in production.

8.4.11 Where the use of mobile code is authorized, configurations will ensure that the authorized mobile code operates according to a clearly defined security standard, and to prevent the execution of unauthorized mobile code when possible.

8.5 Back-up

8.5.1 To maintain the integrity and availability of information and information systems, UOPX IT will ensure that there is a mutually agreeable back-up standard and strategy which aligns with the Disaster Recovery program and Data Retention Policy.

8.5.2 UOPX IT will ensure that back-up copies of information and software are taken and tested regularly in accordance with the agreed back-up standard

8.5.3 Servers in cloud environments that do not contain application data (frequently referred to as "stateless" cloud servers, or "full stack deployment" servers) do not need to be included in the backup program. These servers are never used for recovery purposes. Rather, they are just regenerated from a standard image.

8.6 Network security management

8.6.1 UOPX IT will ensure the secure design, operation, and management of network devices. Access to network devices will be limited to authenticated accounts which have been explicitly assigned for administrative responsibilities. Administrative accounts for all network components will be validated as appropriate no less than once each quarter.

8.6.2 UOPX IT will implement appropriate controls such as strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to protect information traversing public or other untrusted networks.

8.6.3 UOPX IT has sole authority to acquire network equipment and to build and maintain the UOPX network infrastructure, except where IT has delegated specific authority outside of IT. All systems and equipment connected to the UOPX network must be approved by IT, including but not limited to firewalls, switches, hubs, routers and wireless devices. Devices that do not meet the UOPX configuration standards will not be used on the UOPX network, unless authorized through a policy exception.

8.6.4 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.

8.6.5 Direct access from end point devices to datacenter network segments will only be allowed through approved secure access techniques.

8.7 Media / Information handling

8.7.1 UOPX IT will implement controls to prevent unauthorized disclosure, modification, removal or destruction of information assets, and interruption to business activities.

8.7.2 Appropriate encryption will be applied to data being stored on removable media where business process requires such use.

8.7.3 Authorized use of removable media must adhere to security controls as defined in the Removable Media Standard. Removable media may not be connected to or used with any computer that is not owned or leased by the UOPX without explicit permission of the UOPX Information Security.

8.7.4 Regulated and Confidential information will be 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 UOPX Data Protection Standard

8.7.5 Workers are required to dispose of media or documentation containing data when it is no longer required for business or legal reasons. Hard-copy materials containing Regulated and/or Confidential data, including Payment Card Data, will be crosscut shredded, incinerated, or pulped. Storage containers for information to be destroyed will be secured (e.g., locked). Purge, degauss (erase magnetically), shred or otherwise destroy electronic media so that data cannot be recovered.

8.7.6 UOPX IT will ensure that information residing on removable media is disposed of securely and safely when no longer required.

8.8 Exchange of information

8.8.1 UOPX will implement controls designed to maintain the security of information and software exchanged with any external organization. Exchanges of information and software will be governed by formal exchange agreements which will include non-disclosure clauses as appropriate.

8.8.2 Unless expressly stated otherwise in exchange agreements, UOPX IT will apply equivalent levels of data protection for both UOPX and non- UOPX data.

8.9 Electronic commerce services

8.9.1 UOPX IT will ensure the security of electronic commerce services, and their secure use including the integrity of publicly available systems.

8.9.2 All international and domestic Internet domain names must be approved by UOPX Public Affairs, including all existing domain names involved in mergers and acquisitions.

8.9.3 Approved Internet domain names can only be purchased and registered through UOPX Ethics and Compliance.

8.10 Monitoring

8.10.1 UOPX IT will be responsible for monitoring and detecting unauthorized activities and relevant information security events. System monitoring will be used to check the effectiveness of information security controls and to verify conformity to the information security program.

8.10.2 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.

8.10.3 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 of time as prescribed in the Data Retention Policy.

9 Access Control

9.1 Purpose

9.1.1 The purpose of the Access Control policy is to ensure that UOPX information systems are properly protected with appropriate access control measures.

9.2 Business requirement for access control

9.2.1 UOPX information and information systems will be effectively protected from unauthorized access, modification, or disclosure. Authorization to information and information systems will be granted using the principle of role-based access (business need) and in compliance with applicable local, state, federal and international laws and regulations. Existing access and access control rules will be periodically reviewed and approved by relevant data stewards.

9.2.2 Access for critical applications must be reviewed at least quarterly including acknowledgement from the application Product Owner that permissions are appropriate for each user or permissions must be removed/modified.

9.2.3 For non-critical applications, access reviews must be conducted based on the number of Workers with access, the number of Worker changes, and the type of access.

9.2.4 Non-critical application reviews must be performed at least annually.

9.3 User access management

9.3.1 UOPX IT will utilize a formal process to manage the user access lifecycle and to ensure appropriate assignment of user access rights, preventing unauthorized access to information systems, including management of privileged user accounts and access rights.

9.3.2 UOPX IT will establish individual accountability through provisioning processes which issue each Worker a single, unique username and user defined password.

9.3.3 All authentication systems will be constructed in such a way as to effectively preclude unauthorized access. Password length, password strength, difficult to guess passwords, password expiration, password reuse and failed logon attempts will all be used by authentication systems to mitigate risk of unauthorized access.

9.4 User responsibilities

9.4.1 It is essential that all users of UOPX information and information systems be aware of, and comply with, the information security policy and standards designed to prevent unauthorized user access, and compromise or theft of information.

9.5 Networks / Devices / Applications

9.5.1 UOPX IT will prevent unauthorized access to both internal and external networked services by ensuring that appropriate interfaces and security mechanisms are in place to protect and segregate the UOPX network from those networks owned by other organizations and / or public networks.

9.5.2 UOPX IT will prevent unauthorized access to information system devices by restricting access to authorized administrators only. Effective audit mechanisms will be used to monitor for inappropriate use of privileged accounts.

9.5.3 UOPX IT will prevent unauthorized access to information held in application systems by restricting access to and within application systems in accordance with the defined access control policy (10.2) and standards, and by segmenting sensitive applications into dedicated computing environments as appropriate.

9.5.4 Systems that contain regulated information will have an isolated computing environment.

9.5.5 Authentication credentials must be encrypted when stored or transmitted, including over the internal network.

9.5.6 UOPX IT will ensure that accounts and sessions are shut down after a defined period of inactivity.

9.6 Remote Access

9.6.1 All Workers accessing any application in support of UOPX business (e.g. SaaS, on-premise, etc.) are considered an extension of UOPX, and, as such, are subject to all Information Security policies.

9.6.2 UOPX IT will implement and enforce appropriate information security controls for remote access using Virtual Private Networks (VPN).

9.6.3 It is the responsibility of all Workers that have VPN privileges to ensure that unauthorized users are not allowed access to UOPX networks and associated content.

9.6.4 All Workers and systems, while using UOPX VPN technology, are considered an extension of UOPX, and as such are subject to all Information Security policies.

9.6.5 All authorized remote Workers will only access systems and resources that they have permission and rights to use.

9.6.6 External connections provided for use by vendors will only be made available at time of need and must be immediately deactivated after use.

10 Information Systems Acquisition, Development and Maintenance

10.1 Purpose

10.1.1 The purpose of the Information Systems Acquisition, Development and Maintenance policy is to ensure that security is an integral part of the organization's information systems, and of the business processes associated with those systems.

10.2 Security requirements of information systems

10.2.1 UOPX will ensure that information security is an integral part of information systems (operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications). Information security requirements will be identified, justified, agreed and documented throughout the development and/or implementation of information systems.

10.2.2 UOPX will ensure that all appropriate templates and guides for new or enhanced information systems include documentation of security controls as part of requirements definition.

10.3 Correct processing in applications

10.3.1 UOPX will manage errors, loss, unauthorized modification or misuse of information in applications, including those developed in house, by designing appropriate application controls to ensure correct processing. These controls are to include the 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. Additional controls will be determined based on security requirements and risk assessment.

10.3.2 The UOPX development process will include requirements for ensuring authenticity and protecting message integrity in applications, and that appropriate information security controls are identified and implemented.

10.4 Cryptographic controls

10.4.1 UOPX IT will protect information using cryptographic controls and key management for sensitive information at rest or in transit, when required by laws and regulations or when deemed otherwise appropriate.

10.5 Security of system files

10.5.1 UOPX IT will ensure the security of information systems by controlling generation of, and access to system files and program source code.

10.5.2 UOPX IT will ensure that there are procedures in place to control the installation of unauthorized software on operational systems.

10.6 Security in development and support processes

10.6.1 UOPX IT will maintain the security of application system software and information by strictly controlling changes to non-production and production environments. Managers responsible for application systems are responsible for the security of the development environment and must ensure that all proposed changes are reviewed to check that they do not compromise security controls.

10.6.2 UOPX will ensure that all appropriate templates and guides for new or enhanced application development include documentation of security controls as part of requirements definition.

10.6.3 UOPX will ensure that test data is selected carefully, protected and controlled. Where test data is sourced from production, PI data will be removed and anonymized and controls will be in place to ensure that all regulatory and privacy expectations are extended to the test data and the environments in which test data reside.

10.6.4 UOPX IT will ensure that when operating systems are changed, business critical applications are reviewed and tested as appropriate to ensure there are no adverse effects.

10.6.5 UOPX will ensure that modifications to software is strictly managed and controlled.

10.6.6 UOPX will ensure that no modifications are 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.

10.6.7 UOPX IT will ensure that applications are designed and managed in such a way as to prevent information leakage as much as possible.

10.6.8 UOPX IT will ensure that outsourced software development is supervised and monitored, and that all information security controls governing internal development of applications are also extended to third-party developers as well.

10.7 Technical Vulnerability Management

10.7.1 Timely awareness of relevant technical vulnerabilities associated with information systems will be maintained by UOPX IT, who will evaluate the organization's exposure to such vulnerabilities, and will take appropriate measures to address the associated risk.

11 Information Security Incident Management

11.1 Purpose

11.1.1 The purpose of Information Security Incident Management is to ensure information security incidents and weaknesses associated with the UOPX information and information systems are communicated in a manner that allows appropriate corrective actions to be taken.

11.1.2 Incidents involving that might be considered high-visibility or significant must be referred to the Incident Response Plan. For the purposes of guidance, the following are some examples of Incidents:

- Incidents involving key University of Phoenix personnel.
- Incidents for which a press release may or will be issued, or media coverage is anticipated.
- Incidents likely to result in a regulatory reporting obligation.
- Incidents likely to result in litigation or regulatory investigation.
- Incidents involving criminal activity.
- Incidents in which Sensitive Information may have been accessed or acquired without authorization.
- Incidents in which business operations are materially impacted.

11.2 Reporting information security events and concerns

11.2.1 UOPX Information Security Operations is responsible for managing incident response and developing incident response procedures to ensure information security incidents and concerns associated with information systems are communicated in a manner allowing timely corrective action to be taken.

11.2.2 All Workers are required to report any confirmed or suspected information security incident(s) to Information Security.

11.2.3 All Workers are required to report any concerns relating to a flaw or bypass of Information Security policies or standards, to infosec@phoenix.edu.

11.3 Management of information security incidents and improvements

11.3.1 The only personnel authorized to formally declare an Incident and activate the Incident Response Plan is the Chief Information Officer, Vice President, Information Security, and/or Chief Privacy Counsel, or their assigned designee.

11.3.2 UOPX Information Security Operations will ensure that a consistent and effective approach is applied to the management of information security incidents. Logs and other evidence will be collected and retained in accordance with compliance and legal requirements.

11.3.3 UOPX Information Security Operations will ensure a timely and effective response to reported information security incidents.

11.3.4 UOPX IT will ensure that where a follow-up action against a person or organization after an

information security incident involves legal action (either civil or criminal), evidence is available, collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

12 Business Continuity Management

12.1 Purpose

12.1.1 This policy establishes the basic principles and framework necessary to ensure emergency response, continuation, resumption, recovery, restoration and permanent recovery of UOPX operations and business activities during a business interruption event.

13 Compliance

13.1 Purpose

13.1.1 The purpose of the Compliance Policy is to ensure that UOPX is compliant with all statutory, regulatory, certificatory or contractual obligations.

13.2 Compliance with legal requirements

13.2.1 UOPX will ensure effective information security controls are designed and implemented to avoid breaches of any law, statutory, regulatory, and contractual obligation. UOPX IT will solicit advice on specific legal requirements from corporate advisers, or (when directed) suitably qualified legal practitioners.

13.2.2 UOPX will ensure that all relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements are explicitly defined, documented, and kept up to date for each information system and the organization.

13.2.3 UOPX will ensure that appropriate standards and procedures are implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

13.2.4 UOPX will ensure that important records are protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements. See Records Management

13.2.5 UOPX will ensure that data privacy and protection controls are managed as required in relevant legislation, regulations, and, if applicable, contractual clauses.

13.3 Compliance with security policies and standards, and technical compliance

13.3.1 UOPX will ensure compliance of information systems through ongoing control owner attestation and by regularly auditing for compliance with information security policies, standards and documented controls.

13.4 Information systems audit considerations

13.4.1 UOPX will maximize the effectiveness of the information systems audit process by ensuring there are controls to safeguard audit tools used for information systems audits. Controls will also be provided to safeguard the integrity and prevent misuse of audit tools.

13.4.2 UOPX will ensure that audit requirements and activities involving checks on operational systems are carefully planned and scheduled to minimize the risk of disruptions to business process.

14 Policy Background Information

14.1 Origin in ISO/IEC 27001 and appropriate NIST controls

14.1.1 In line with senior management guidance, this manual reflects ISO/IEC 27002:2013, an international information security management standard. These were reviewed to match the UOPX situation and adapted to suit the style of this manual. Secondly, we selected from ISO/IEC 27002 and other sources a range of supporting security controls that we believe will satisfy these control objectives. The supporting controls are not explained in detail in these policy statements. Rather, more detailed control content can be found in information security standards, and procedures. However, these policy statements are intended to provide sufficient direction to reinforce the need for particular controls, under management's mandate.

14.1.2 Consideration has been given for alignment to applicable NIST controls identified in NIST 800-53a (Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans) and NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).

14.2 Formatting and presentation

14.2.1 The sections of this manual contain several formal purpose statements, policy statements, and links to standards describing the supporting controls and supplementary guidance. Policy statements are derived directly from the control objectives stated in ISO/IEC 27002. The ISO/IEC 27002 controls have been explicitly approved by the Corporate Policy Governance committee.

14.2.2 Throughout the manual, the words "will" or "must" imply an absolute compulsion i.e. the stated policies and controls are mandatory or obligatory, unless exceptions have been explicitly agreed by senior management.

14.2.3 The manual contains numerous examples, usually preceded by "e.g." The examples are not intended to be exhaustive, merely illustrative.

14.3 References

14.3.1 Just like ISO/IEC 27001, this policy incorporates internal cross-references since certain controls are relevant to more than one section. The definitive online version of this policy on the Intranet contains fully functional hyperlinks.

15 Revision Log

Author	Date	Description	Reviewer	Approver	Version
M. Hernandez	01/08/2015	Revisions and updates	InfoSec	Bill Smathers	1.7
M. Hernandez	01/22/2016	Revisions and updates	InfoSec	Bill Smathers	1.8
S. Geyer	08/24/2016	Reformatted, updated links	InfoSec	Bill Smathers	1.9
S. Geyer	07/12/2017	Reformatted, updated links	InfoSec	Bill Smathers	2.0
	02/01/2018	Repaired broken link			
L. Schwarberg	12/30/2019	Updated outdated information in all sections	InfoSec		2.1
L. Schwarberg	4/2/2020	Updated formatting and content	InfoSec	Corporate Policy Group	2.2