University of Phoenix®

Information Security Standard

Third Party Security

November 3, 2017
Version 3.2

Internal Use Only

TABLE OF CONTENTS

1 Purpose

Presented within this document are information security requirements, policies, and standards for vendor companies that render services to University of Phoenix and/or have access to UOPX Assets.

2 Scope

This standard establishes guidelines, practices, and requirements for vendor company responsibility while providing services to UOPX. Subject matter includes: Requirements for all Companies, Organization of Information Security, Risk, Asset Management, Human Resources Security, Operations Management, Access Control, requirements, policies, and standards relevant to Information Security.

3 Third Party Information Security Standards

3.1 General requirements for access to UOPX assets

3.1.1 If a company has access to UOPX assets, that company must handle, treat, and otherwise protect UOPX assets in accordance with all requirements, policies, standards, processes and procedures set forth in this policy and any contractual agreement between such company and University of Phoenix.

3.1.2 If a company is found to be High risk, an annual review of their security controls is required.

3.1.3 A SOC 2 report is required for all service providers.

3.2 Resolving conflict between policy and written contract terms

3.2.1 If there is a direct conflict between any term of this policy and the terms of a written contract between company and UOPX, the terms of the written contract will prevail to the extent of the conflict.

3.3 Requirements for all Companies

3.3.1 Information Security Risk Management

3.3.1.1 Companies must periodically assess risk within Information Technology (“IT”) that accesses UOPX assets.

3.4 Information Security Policy

3.4.1 Security Program Requirements:

Companies must have a documented and followed Information Security program that is based on at least one of the following Information Technology industry leading security frameworks, such as:

a. International Organization for Standardization ("ISO") 27001
b. Information Security Forum ("ISF") Standards of Good Practice ("SoGP")
c. National Institute of Standards and Technology ("NIST") Special Security Publications

3.5 Security Program Framework

3.5.1 Companies must map their security program to one of the above security frameworks. Maps must not show any gaps in company security programs.

3.6 Organization of Information Security

3.6.1 Companies must define, document and assign ownership to oversee development, adoption, enforcement and compliance with Information Security requirements, policies, standards and procedures

3.6.2 Companies must ensure the assigned role must be of a sufficiently high-level classification in the organization that can be allowed to execute the responsibilities in an effective and independent manner.

3.7 Conflict of Interest

3.7.1 Companies must avoid conflict of interest. To avoid conflicts of interest, companies must ensure information security roles will not have direct responsibility for information processing and technology operations.

4 Asset Management

4.1.1 Companies must maintain a current inventory of company's assets that access UOPX assets.

4.1.2 Companies must document and implement rules for the acceptable use of assets of third parties, including without limitation, UOPX assets.

4.1.3 Acceptable use requirements:

a. Rules of acceptable use must require that third party assets are not to be used for activities which have been identified as unacceptable conduct.
b. Rules of acceptable use must require that third party Assets are to be used in a professional, lawful and ethical manner.

4.1.4 All Companies who connect to or use an UOPX Asset (including servers, workstations, infrastructure, internet gateway or network) must abide by all applicable UOPX terms of use, and any supporting standards and procedures.

4.1.5 Companies are required to safeguard and use UOPX assets wisely and apply good judgment and discretion when using UOPX assets:

a. UOPX systems
b. Voice mail
c. Fax machines
d. Computers
e. Email
f. Telephones
g. Copiers
h. Internet access
i. Vehicles
j. Or other property

4.1.6 Companies must never connect non-UOPX owned assets to the UOPX corporate network without direct written approval from UOPX Information Security.

4.1.6.1 Approved assets that connect to UOPX network must still abide by UOPX security standards, operating practices and controls including, but not limited to:

a. Virus protection processes
b. Hardening
c. Patching
d. Access Control

5 Human Resources Security

5.1.1 Companies must ensure all Company employees and Company subcontractors who access UOPX Assets are screened prior to employment. Screening must include criminal, financial, employment background screening processes.

5.1.2 Company must have processes in place to periodically screen personnel during employment for anyone who accesses UOPX Regulated, Confidential or Personal Information.

5.1.3 Companies must ensure an Information Security awareness campaign is provided to anyone who accesses UOPX assets. Company must educate personnel of their responsibilities to secure UOPX assets.

5.1.4 Companies must ensure all User IDs, tokens or physical-access badges are assigned to a unique Company employee or Company subcontractor.

5.1.5 Companies must ensure all user/system/service/administrator accounts which have access to UOPX assets and passwords are never shared.

5.1.6 When access to UOPX assets is managed by the vendor, they must immediately remove access to UOPX assets for any employees who are terminated, or no longer require access to UOPX assets.

5.1.7 When access to UOPX assets to UOPX assets are managed by UOPX, the vendor must immediately advise UOPX in writing when vendor employees have been terminated or should no longer have access to UOPX assets. Notices must include name, User ID name of any accounts the person had access to or knows the password.

6 Physical and Environmental Security

6.1.1 Company must store UOPX assets in locations that are protected from:

a. Natural Disasters
b. Heat or Cooling Problems
c. Ventilation
d. Theft
e. Power failures or outages
f. Physical intrusion
g. Unlawful and unauthorized physical acces

7 Operations Management

7.1 Network security

7.1.1 Companies must deploy Data Leakage Prevention (“DLP”) and or Intrusion Monitoring Services at perimeter points where UOPX Regulated, Confidential or Personal Information is used.

7.1.2 Companies must ensure all unnecessary services, ports and network traffic are disabled on all IT systems that access UOPX Assets.

7.2 System Security

7.2.1 Companies must have a process for applying and managing security updates, patches, fixes, upgrades, (collectively referred to as “Patches”) on all Company IT systems.

a. Companies must ensure patches that provide security fixes and updates are deployed within 30 days of manufacturer’s release on all IT systems that access UOPX Confidential, Personal, or Regulated Information.

b. Otherwise, companies must ensure patches that provide security fixes and updates are deployed within 120 days from a manufacturer release on all IT systems that access UOPX assets.IPS and software firewalls must have the latest and up-to-date manufacture's signatures, definition files, software patches.

7.2.1.1 Software firewalls must be configured to monitor and block unauthorized traffic.

7.2.1.2 HIPS (host-based intrusion prevention) must be configured to monitor and block threats and unauthorized software.

7.2.1.3 HIPS and Software firewalls must be configured to report all unauthorized activity to a secure central repository that retains records for up to one year.

7.2.1.4 If requested by UOPX, Company must provide logs of all unauthorized activity captured in HIPS, software firewalls, and any other log files.

7.2.2 Companies must ensure all unused or unnecessary software, applications, services, sample/default files and folders are disabled on all IT systems that access UOPX assets.

7.3 Data Security

7.3.1 Companies must use strong encryption key management practices to ensure the availability of encrypted authoritative information.

7.3.2 Companies must encrypt all UOPX digital assets in transmission between company and UOPX, and between company and all external sources. External sources include UOPX's business partners and subcontracting companies and Companies' business partners and subcontracting companies.

7.3.2.1 Companies must encrypt Regulated Information at rest at all times.

7.3.2.2 Encryption must meet minimal standards of 168 bit encryption.

8 Operation Security

8.1.1 Companies must ensure that any changes to IT systems that are performing work on or for do not have any negative security implications.

8.1.2 Companies must follow documented change management procedures.

8.1.3 Companies are restricted from transferring Regulated, Personal or Confidential Information to any non-production environment or insecure location.

9 Access Control

9.1.1 Companies must ensure controls restrict company's other customers from accessing UOPX data.

9.1.2 Companies must use authentication and authorization technologies for all accounts that access UOPX data. Unless approved in writing by Information Security, Companies must not allow UOPX or Company employees or subcontractors direct root access to any systems or access to the administrator user account.

Note: For UNIX or UNIX-like Operating systems, users must use the "sudo” command where all access must be logged.

9.1.3 Companies must ensure IT administrators are using separate and unique administrator accounts that are only used for administration responsibilities. Non-administration tasks must always be performed using non- administrator user accounts.

9.1.4 Companies must ensure password policies and standards exist on IT systems that access UOPX assets.

9.1.5 Companies must ensure systems that access Confidential, Personal or Regulated Information require the following password construction requirements at all times:

a. Minimum length: 8 characters
b. Complexity: Must contain at least three of the following four characters:
   - Number
   - Uppercase letter
   - Lowercase letter
   - Printable special character
c. History (reuse): >. 10 passwords
d. Expiration: <= 90 days — including system administrators
e. Service account passwords must be changed at least annually
f. Failed login attempts: <= 6 attempts
g. Account lockout: > 29 minutes
h. Screen saver locks must be enabled: <= 15 minutes for OS and <= 30 minutes for applications containing sensitive information

9.1.6 Companies must ensure procedures exist for provisioning priviledged accounts.

9.1.7 Companies must periodically review users of priviledged accounts to verify access is still appropriate and necessary to each users role.

9.1.8 If a company requires remote access to UOPX assets, that Company must always use a UOPX approved method to remotely connect to any UOPX asset.

9.1.9 Companies must ensure systems that access UOPX assets meet the following additional requirements at all times:

a. Authentication credentials must be encrypted when stored or transmitted at all times.
b. Passwords for user-level accounts cannot be shared between multiple individuals
c. Companies must change their passwords immediately whenever it is believed that an account may have been compromised.
d. Passwords must not be communicated via email messages or other forms of electronic communication, other than one-time use passwords.
e. Passwords for individual user accounts must never be given to, or shared with, someone other than the account owner.
f. A user’s identity must be verified before their password is reset and an email or voicemail notification must be sent to notify the user their password was reset.

g. First-time passwords for new user accounts must be set to unique values that follow the requirements set forth in this standard and must not be generic, easily-guessed passwords.

h. User accounts must be configured to force a change of their password upon first use of a new account or after a password is reset.All manufacturer passwords must be changed from their default values (including when the default value is NULL) and must meet the requirements set forth in this standard. Manufacturer passwords include, but are not limited to, SNMP community strings, system-level administrator account passwords, temporary account passwords, wireless encryption keys, and other default authentication settings.

i. Password fields must display only masked characters as the user types in their password, where technically feasible.

j. Hardcode plain-text passwords must not be used in production environments.

k. Production account passwords must not be used in non-production environments.

l. If a system-level administrator account (e.g. Windows local administrator or UNIX/Linux root) is used to perform privileged management of a device, that password must be changed following completion of that management task.

m. If an account has a machine-set complex password of 20 characters or more that is never accessed or known by a human, that password does not need to be changed during its lifetime, unless the account or its associated system has been suspected of compromise.

n. System-level account passwords must be unique on each device.

o. Service-level accounts may be set to never lock out due to failed login attempts and do not need to enforce password expiration.

p. All systems must prompt users to re-authenticate when users attempt to elevate their privileges to higher security levels. Examples include use of sudo or su on UNIX/LINUX systems or “run as” for Microsoft Windows based systems.

9.1.10 Companies must ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.

9.1.11 If a Company requires remote access to UOPX assets, that Company must always use a UOPX approved method to remotely connect to any UOPX asset.

10 Information Technology Acquisition, Development and Maintenance

10.1 Vulnerability Assessments

10.1.1 Companies must ensure Infrastructure, network and application vulnerability assessments are periodically conducted and follow industry acceptable vulnerability management practices (e.g. processes described in NIST & OWASP).

10.1.2 Companies must ensure industry acceptable application development security standards (e.g. OWASP) are followed so that IT systems and applications are tested and secured in every step of the application and system development life cycle.

10.1.3 Companies must ensure firmware, software and application source code are validated and tested against vulnerabilities and weaknesses before deploying to production.

10.1.4 Companies must ensure security incident response planning and notification procedures exist to monitor, react, notify and investigate any incident related to an UOPX assets.

10.1.5 Once Companies discover or are notified of a security breach, Companies must investigate, fix, restore and conduct a root cause analysis.

10.1.6 Companies must provide UOPX with results and frequent status update of any investigation related to UOPX.

10.1.7 If UOPX is not satisfied with the speed or effectiveness of investigation, Companies must include UOPX Information Security staff in the investigation and response teams.

10.1.8 Company will work with UOPX to address any concerns.

10.2 Business Continuity Management

10.2.1 When required by UOPX, Company and UOPX must document and agree to an achievable and tested Recovery Time Objectives (RTOs).

10.2.2 Company must maintain a comprehensive and current Business Continuity Plan ("BCP") that documents processes and procedures that are implemented to ensure essential business functions continue to operate during and after a disaster, and a Disaster

10.2.3 Disaster Recovery Plan ("DRP") that documents technical plans for specific restoration of UOPX processes and assets according to published RTOs.

10.2.4 BCP and DRP must be updated after function, process, or IT changes.

10.2.5 Summary results of DRP and BCP tests must be provided to UOPX if requested.

10.2.6 Upon request, Companies must include UOPX Information Security staff in the investigation and response teams.

11 Compliance

11.1 Data Security

11.1.1 Data destruction processes must follow result in a secure wipe of all data on all media rendering the data incapable of being retrieved. For all IT systems that access Regulated,Confidential, or Personal Information, UOPX requires the destruction be performed in accordance with NIST Special report 800-88, Gutmann Method, US DoD 5220-22.M

11.1.2 If requested by UOPX, company must provide adequate validation of any subcontracted company is compliant with this document.

11.1.3 Company must obtain written permission from the UOPX Legal Department to move UOPX assets across any international borders.

11.1.4 If applicable, Companies must secure all Credit Card data in accordance to requirements listed in the most current and released editions of the Payment Card Industry – Data Security Standards (“PCI-DSS” or “PCI”).If applicable,

11.1.5 Companies that access Credit Card data must annually provide evidence of PCI certification/compliance.

11.2 Additional Requirements for Hosting Service Providers

11.2.1 In addition to all requirements listed above, the following requirements must be followed by all Companies who provide hosting services to UOPX. Hosted services include, without limitation, cloud computing or offsite hosting services. Cloud computing can be Company service offerings that allow UOPX to dynamically lease and provision Infrastructure, Virtual Environments, Platforms and Software.

11.2.2 In the event the company's hosting service model shifts some responsibility of the below requirements to UOPX, the Company must still complete a "Policy Exception Request" as defined in 12.2 of this document to clearly define ownership or responsibility. UOPX will not assume any ownership for any requirement below without a direct agreement listed in a written contract, statement of work or an UOPX approved Policy Exception Request.

11.2.3 Companies that provide hosting services are responsible for all requirements below.

11.3 Operations Management

11.3.1 Company to ensure UOPX asset protection.

11.3.1.1 Companies who provide Infrastructure and Platform hosting services must ensure Non-UOPX authorized personnel cannot physically or electronically:

a. Inspect
b. Share
c. Steal
d. Access
e. Change content to

UOPX assets, including:

a. UOPX used network
b. Applications
c. Traffic
d. RAM
e. Infrastructure
f. Storage space

11.4 Network Security

11.4.1 **Network Security:** Within UOPX used or leased services, Companies must restrict by protocol, service port and source IP address, and MAC address through the use of firewall technologies

11.4.2 Companies must ensure firewalls are configured with different policies that allow UOPX used Web Servers, Application Servers and databases are protected with different levels of security.

11.4.3 Companies must ensure network segmentation and firewall restrictions exist so that UOPX used database servers can only communicate with the following:

a. Application servers located in an Application Virtual Local Area Networks (VLANs)
b. Management Tool Servers located in Management Tool VLANs
c. Network Administration Users located in Admin VLANs

11.4.4 Companies must ensure network segmentation and firewall restrictions exist so that UOPX used application servers can only communicate with the following:

a. Web servers located in Web VLANs
b. Databases located in database VLANs
c. Management Tool Servers located in Management Tool VLANs, and,
d. Network Administration Users located in Admin VLANs
e. Companies must use additional security protection controls for protecting against access to UOPX Regulated, Personal, or Confidential Information, such as:

11.4.5 Companies must use additional security protection controls for protecting against access to UOPX Regulated, Personal, or Confidential Information, such as:

a. Web Application Firewalls
b. Intrusion Prevention Systems
c. Intrusion Detection Systems
d. Data Loss Prevent Systems

11.4.6 Companies must ensure Web Server, App Servers and databases administrative functions are only accessed via SSH or a secure method that encrypts traffic during transmission.

11.5 System Security

11.5.1 Companies must ensure UOPX Assets reside on separate physical hardware from other service provider customers including data distributed in different environments (e.g. backup media, production, development, test, quality assurance, disaster recovery) when transferring or storing UOPX Regulated, Personal, or Confidential Information.

11.5.2 For services that leverage Virtual Environments (VE), Companies must ensure that VEs:

a. Use UOPX standard builds or UOPX approved builds,
b. Company provided platform, build, standard image, or related template for guest operating systems, are validated by UOPX to ensure security requirements are correctly integrated.

c. OS patches are easily deployable to all un-patched servers and applications so that all servers can comply with UOPX patch management standards.
d. VE specific security mechanisms embedded in hypervisor APIs are utilized to provide granular monitoring of traffic crossing VE backplanes, which will be opaque to traditional network security controls.
e. Administrative access and control of VE operating systems include strong authentication integrated with enterprise identity management, as well as tamper-proof logging and integrity monitoring tools.
f. Are segregated in security zones by type of usage (e.g., desktop vs. server), production stage (e.g., development, production, and testing) and sensitivity of data (e.g. UOPX regulated data) on separate physical hardware components such as servers, storage, etc.
g. Have a reporting mechanism in place that provides evidence of VE isolation and raises alerts if there is a breach of isolation.
h. Have capability for File Integrity Monitoring (FIM) to be deployed on VEs to alert on critical file changes.

11.6 Configuring and filtering inbound / outbound traffic

11.6.1 Companies must configure and filter inbound and outbound traffic per instance using host-based firewalls.

11.7 Data Security

11.7.1 Company must encrypt data at rest and in transit in accordance to all regulatory bodies (e.g. PCI), local and national laws (examples are, but are not limited to the following: HIPPA, SOX, GLBA, etc.).

11.7.2 Company must sign and encrypt API requests.

11.8 Operations Security

11.8.1 Company must ensure that when objects are deleted, all mappings to the objects are also removed.

11.8.2 Company must ensure that when domains, objects and trusts are deleted, all mappings to the domains, objects and trusts are also removed.

11.8.3 Company must provide UOPX with the ability to monitor and review critical files for changes or tampering.

11.8.4 Access Control: For systems that access UOPX classified Confidential, Personal or Regulated Information, Company must deploy and offer token or key-based authentication to improve authentication controls.

12 Enforcement and Exceptions

12.1 Enforcement

12.1.1 The UOPX Third Party Information Security Standard is in place to assist UOPX in complying with best practices and legislative and regulatory requirements. Compliance is a task for everyone, including every employee, contractor, consultant, and Company.

12.1.2 This document can be amended with or without notice from time to time in UOPX's sole and absolute discretion. Companies will not be expected to comply with any changes to this document until they have been provided with such changes in writing and a reasonable period (not to exceed 120 days) to comply with such changes.

12.2 Exceptions

12.2.1 In certain specific circumstances it may not be feasible to comply with all content documented in this standard. In such cases, it is critical to obtain prior approval of an exception to this policy. If UOPX approves the non-compliance, the company must document and maintain a record of such instance.

12.2.2 Specifically, if a Company cannot comply with a requirement listed in this document, the sponsoring VP must submit a Policy Exception Request and follow the Policy Exception Request process to gain written approval from UOPX's Information Security Department

13 Definitions

a. **Asset:** Includes, but is not limited to: 1. Information, such as data, databases, hosted data, computer files, documentation, manuals, plans and audit logs
2. Software, such as application and system software, and, 3. Physical equipment, such as computer hardware, peripheral devices and communication.

b. **Company** For the purpose of this policy, Company will be defined as any non-UOPX owned entity that provides products or services to UOPX, including but not limited to third party service providers and Vendors.

c. **Confidential Information**: All confidential and proprietary information of UOPX and includes Personal Information.

d. **InfoSec**: “Information Security Department” - The specific department in UOPX’s Information Technology Services (ITS) division responsible for the governance of UOPX Information security policies, standards, procedures and processes.

e. **ISF:** “Information Security Forum” is an international, independent, non-profit organization dedicated to benchmarking and identifying good practice in information security.

f. **ISO:** “International Organization for Standardization” is an international-standard-setting body composed of representatives from various national standards organizations.

g. **NDA:** Non-Disclosure Agreement

h. **NIST:** “National Institute of Standards and Technology” is a measurement standards laboratory, which is a non-regulatory agency of the United States Department of Commerce.
i. **OWASP:** Open Web Application Security Project
j. **Personal Information:** Any information that a Company obtains in any manner from any source during or in connection with its performance of services for UOPX that concerns any of UOPX prospective, former and existing students, customers or employees. Personal Information includes, without limitation, names, addresses, telephone numbers, e-mail addresses, social security numbers, credit card numbers, call-detail information, student records, purchase information, product and service usage information, account information, credit information, demographic and any other personally identifiable information
k. **Priviledged Accounts:** An account which provides elevated access and requires additional authorization. Examples include a network, system or security administrator account.
l. **Regulated Information:** Personal Information or Confidential Information that requires the greatest degree of controls and safeguards to ensure compliance with state, federal or international law, rule, regulation or ordinance. Examples include, but are not limited to; Credit Card information, Debit Card information, Bank Account information, Social Security Number, Student Records, Protected Health Information, etc.
m. **SNMP:** Simple Network Management Protocol - one of the primary protocols used to gather data about systems.
n. **VRA:** Vendor Risk Assessment
o. **SSH:** Secure Shell - Industry-standard protocol for securing communications

14 Document Associations

Document	Version	URL
Vendor Risk Management	N/A	VendorRiskManagement@phoenix.edu

15 Revision Log

Author	Date	Description	Reviewer	Approver	Version
Information Security	12/13/2010	Released Edition	Information Security	Information Security	1.0
C. Cupone	808/06/2013	Revision and updates	C. Cupone	B. Smathers	2.0
A. Charad	08/26/2015	Revision and updates	M. Hernandez	B. Smathers	3.0
S. Geyer	09/23/2016	Updated format, links	S. Geyer	B. Smathers	3.1
S. Geyer	11/3/2017	Rebranded and updated for UOPX	S. Geyer	B. Smathers	3.2