INFORMATION RISK MANAGEMENT PROGRAM

Unit Privacy Coordinator (UPC) Tasks

Information Security & Privacy Office

July 7, 2017

Version 1.6
The Unit Privacy Coordinator (UPC) manages a unit's privacy program to meet university policy objectives.

UPCs help unit faculty, staff, and management protect university information classified as protected or private by implementing methods dictated by recommended business practices, university policy, rules, regulations, or contractual obligations.

The dean, director, or department head assigns the UPC role. The person designated with the UPC role does not need to have a technical background. Administrative staff, data owners, associates in research, and coordinators are prospective candidates.

The amount of time required to fulfill UPC tasks will vary based on the complexity of the unit’s information infrastructure and the information that must be secured. For example, certain unit business processes may require higher allocations of time to meet select privacy obligations such as The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This document covers the basic functions of the UPC as outlined in the FSU Information Privacy Policy 4-OP-H-12.
1. **Maintain the information identification and classification documentation of unit protected and private information assets**

The UPC works with users, data owners, data custodians (IT Systems Administrators) and business/function owners to determine the classification required for data and information applications that support unit business processes. If data from enterprise systems (e.g., OMNI, Campus Solutions, Blackboard/Canvas, or building access systems) is downloaded and used locally, that data should be included in the unit inventory. Likewise, vendor contracted cloud based applications used by the unit also should be documented and classified. Units with an emphasis on research need to ensure the unit inventory includes research and intellectual property supporting applications. Information and supporting systems classified are to be identified on the ISPO Privacy Worksheet. Additional information is entered in applicable worksheet columns to assist in the risk analysis process.

**Resources:**

A. [University Information Classification Guidelines](#) – Provides instructions for classifying different data and information items based on policy, rules, regulations, and contractual obligations.

B. ISPO Information Inventory Worksheet - Excel based spreadsheet providing a standardized format to log data/information, applications, specific details concerning data/information, and assigned privacy risk to the unit should unauthorized access occur.
2. Assess the unit’s electronic and physical controls for protected or private information to ensure they meet requirements.

Information/data and system privacy reviews are vital to the privacy risk management process. The UPC works with users, data owners, data custodians, and management to review university policy, rules/legislation, and contractual obligations against the data/information collected on the information inventory worksheet. Data owners and data custodians should compare current logical and physical controls to the appropriate legal or contractual obligations to document any control gaps. A control mitigation program is instituted to correct any discovered gaps. Non-technical UPCs should rely on data owners and technical staff to provide the supporting information to meet this task. ISPO supports enterprise funded tools such as Nexpose, RPT Privacy Policy Tester, and Spirion’s Data Platform to assist unit administrators in risk discovery and mitigation tasks.

Resources:

A. ISPO Information Inventory Worksheet  
B. Nexpose Vulnerability Scanner (ISPO Supported-PC/Laptop/Server/Tablet/Network Equipment)  
C. RPT Privacy Policy Tester (ISPO Supported-Website Protected/Private Information Discovery Tool)  
D. Spirion’s Data Platform (ISPO Supported-Server/PC/Tablet Protected/Private Information Discovery Tool)  
E. Fluke Wireless Analyzers (ISPO Supported-Rogue wireless detection)  
F. University Privacy Policy / University Security Policy  
G. ISPO Risk Management Survey/Questionnaire  
H. Security.fsu.edu>Support Resources (links to select privacy legislation and contractual information including HIPAA, FERPA, GLBA, Human Subject Research)
3. Ensure unit staff are trained on the Information Privacy Policy, and specific legislated or contracted privacy requirements.

The UPC works with management, data owners, and systems administrators to identify and train individuals handling protected or private information. While ISPO provides select training resources to assist in meeting this requirement, it is the responsibility of the UPC to mitigate any training gaps. Specialized training to meet a specific rule, regulation, or contractual obligation may have to be obtained through local unit efforts or vendors providing specialized training resources. In addition, any method used to support training should allow the audit of employee completion of training tasks. Documentation may be either in an electronic or paper format. Select legal or contractual provisions may dictate the length of time these records are maintained.

**Resources:**

A. University Information Privacy Policy  
B. University Information Security Policy  
C. ISPO Provided “Securing the Human” IT Security Awareness Video Training  
D. Federal Virtual Training Environment-Free Training  
E. FSU FERPA Training PowerPoint  
F. FSU Registrar FERPA Information Website  
G. Florida Information Protection Act 2014 PowerPoint  
H. Office of Research-Protection of Research Subjects/Human Subjects  
I. Security.fsu.edu>Support Resources (links to select privacy legislation and contractual information including HIPAA, FERPA, GLBA, Human Subject Research)
4. Ensure all unit personnel, e.g., faculty, staff, and students who handle protected or private information sign an Employee Statement of Understanding Regarding Confidentiality.

The UPC works with unit HR/Compliance administrators to ensure all personnel handling protected or private information have a signed/acknowledged statement on file. This can be either a paper-based system or electronic; however, either system must be auditable.

Certain rules, laws, or legislation may require an additional employee confidentiality statement. An example is for The Health Insurance Portability and Accountability Act of 1996 (HIPAA) which requires a HIPAA confidentiality agreement not associated with the general FSU agreement.

**Resources:**

A. [FSU Employee Statement of Understanding Regarding Confidentiality](#)

B. Local Unit Privacy/Confidentiality statement to meet legal or contractual obligation (HIPAA, etc.)
5. Works with legal resources to ensure contracts and agreements stipulate adherence to FSU policy, federal and state laws, and contractual safeguarding provisions when protected or private information is processed, transmitted, or stored by a third-party vendor.

Per FSU’s Privacy Policy, contracts and agreements for the transfer of protected or private university information to Internet or cloud-based service providers and internally hosted systems and solutions maintained by vendors must attach the university’s IT security and privacy addendum and incorporate its provisions by reference. FSU Procurement has attached the Terms and Conditions to all Purchase Orders to facilitate compliance; however, it is still up to the UPC to ensure that vendor actions or contract terms do not result in removing the Terms and Conditions from the final agreement. It is important for the UPC to be involved in unit IT procurement services to ensure that required protections are in place and that responsibilities are clearly delineated.

If a vendor refuses to include the FSU security and privacy addendum, the UPC should seek assistance from FSU legal resources and the Information Security and Privacy Office.

**Resources:**

A. [Contract Addendum for University Sharing of any Information Classified as Protected and Private with a 3rd Party Vendor or Service Provider](#)
Florida State University INFORMATION
SEcurity and Privacy
Standard Terms and Conditions

April 20, 2017

These Information Security and Privacy terms and conditions are hereby incorporated in and attached to Agreements or Contract by and between Florida State University Board of Trustees (University) and Contractor by reference. Contractor agrees to include all of the terms and conditions contained in this URL in all subcontractor or agency contracts providing services under said Contract.

Contractor acknowledges that its performance of Services under the Contract may involve access to confidential University information including, but not limited to, personally--identifiable information, student education records, protected health information, or individual financial information (collectively, “Protected or Private Information as noted in the University’s Information Classification Guidelines”) that is subject to state or federal law/rules restricting the use and disclosure of such information, including, but not limited to; the federal Gramm-­‐-­‐­‐­Leach-­‐­‐­‐­‐­Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)); the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); and the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act; the Payment Card Industry Data Security Standards (PCI DSS); International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR); Federal Trade Commission Red Flags Rule and Social Security Act. Contractor agrees to comply with all applicable state or federal law or contract or agreements restricting the access, use and disclosure of Protected Information. Contractor agrees to include all of the terms and conditions contained in all subcontractor or agency contracts providing services under this Agreement.

Contractor shall not use, access, or disclose University information in any manner that would constitute a violation of state or federal law or contract or agreement terms including, without limitation, by means of outsourcing, sharing, retransfer, access, or use—to any person or entity, except:

a. Employees or agents who actually and legitimately need to access or use University Data in the performance of Contractor’s duties under this Agreement or the Contract;

b. Such third parties, such as but not limited to, subcontractors, as may be specifically identified in this Agreement or the Contract, but only after such third party has agreed in writing and in advance of any disclosure, to be bound by all of the terms of this Agreement;
c. Any other third party approved by the University in writing and in advance of any disclosure, but only to the extent of such approval.

I. **COMPLIANCE WITH FAIR INFORMATION PRACTICE PRINCIPLES**

With respect to the University’s Protected or Private Information, and in compliance with all applicable laws and regulations, **Contractor** shall comply in all respects reasonably pertinent to the Agreement with the *Fair Information Practice Principles*, as defined by the U.S. Federal Trade Commission (http://www.ftc.gov/reports/privacy3/fairinfo.shtm). If collecting Protected or Private Information electronically from individuals on behalf of the University, **Contractor** shall utilize a privacy statement or notice in conformance with such principles (the University’s sample Privacy Statement for websites is available at http://fsu.edu/misc/policy.html).

II. **PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF PROTECTED INFORMATION**

**Contractor** agrees to hold the University’s Protected or Private Information, and any information derived from such information, in strictest confidence. **Contractor** shall not access, use or disclose Protected or Private Information except as permitted or required by the Agreement or as otherwise authorized in writing by University, or applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected of Private Information, **Contractor** will notify University in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give University an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Any transmission, transportation or storage of Protected or Private Information outside the United States is prohibited except on prior written authorization by the University.

III. **SAFEGUARD STANDARD**

**Contractor** agrees to protect the privacy and security of University data designated as Protected or Private Information in full compliance with any and all applicable laws, regulations, rules or standards, including, but without limitation, FERPA, HIPAA, GLB, the Federal Trade Commission Red Flags Rule, EAR, ITAR, the Social Security Act, and PCI----DSS. **Contractor** shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality (authorized access), integrity and availability of the Protected or Private Information. While **Contractor** has responsibility for the Protected or Private Information under the terms of this agreement, **Contractor** shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities.

- All facilities used to store and process Protected or Private Information will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure **Contractor’s** own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.

- Without limiting the foregoing, **Contractor** warrants that all Protected or Private
Information will be encrypted in transmission (including via web interface) and may require encrypted storage at no less than 128bit level encryption.

- **Contractor** will use industry standard and up-to-date security tools and technologies such as antivirus protections and intrusion detection methods in providing Services under this Agreement.

**Contractor** shall not store or process University Protected or Private Information outside of data centers located in the United States.

**IV. RETURN OR DESTRUCTION OF PROTECTED INFORMATION**

Within 30 days of the termination, cancellation, expiration or other conclusion of the Agreement, **Contractor** shall return the Protected or Private Information to University in an agreed upon format, unless the University requests in writing that such data be destroyed. This provision shall also apply to all Protected or Private Information that is in the possession of subcontractors or agents of **Contractor**. Such destruction shall be accomplished by “purging” or “physical destruction” in accordance with commercially reasonably standards for the type of data being destroyed (e.g., *Guidelines for Media Sanitization*, NIST SP 800---88). **Contractor** shall certify in writing to University that such return or destruction has been completed.

**V. BREACHES OF PROTECTED INFORMATION**

**Definition.** For purposes of this article, the term, “Breach,” has the meaning given to it under the applicable Florida (F.S. 501.171), applicable state or federal rule/regulation, or contractual obligation.

**Reporting of Breach.** Immediately upon discovery of a confirmed or suspected Breach, **Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than two (2) business days after **Contractor** knows or reasonably suspects a Breach has or may have occurred. In the event of a suspected Breach, **Contractor** shall keep the University informed regularly of the progress of its investigation until the uncertainty is resolved.

**Contractor’s** report shall identify:

(i) The nature of the unauthorized access, use or disclosure,
(ii) The Protected or Private Information accessed, used or disclosed,
(iii) The person(s) who accessed, used and disclosed and/or received Protected or Private Information (if known),
(iv) What **Contractor** has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and
(v) What corrective action Contractor has taken or will take to prevent future unauthorized access, use or disclosure.
(vi) Contractor shall provide such other information, including a written report, as reasonably requested by University.

Coordination of Breach Response Activities. In the event of a Breach, Contractor will:

• Immediately preserve any potential forensic evidence relating to the breach;
• Promptly (within 2 business days) designate a contact person to whom the University will direct inquiries, and who will communicate Contractor responses to University inquiries;
• As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore University service(s) as directed by the University, and undertake appropriate response activities;
• Provide status reports to the University on Breach response activities, either on a daily basis or a frequency approved by the University;
• Coordinate all media, law enforcement, or other Breach notifications with the University in advance of such notification(s), unless expressly prohibited by law;
• Make all reasonable efforts to assist and cooperate with the University in its Breach response efforts; and
• Ensure that knowledgeable Contractor staff are available on short notice, if needed, to participate in University---initiated meetings and/or conference calls regarding the Breach.

Costs Arising from Breach. In the event of a Breach by the Contractor or its staff, Contractor agrees to indemnify and hold harmless the University arising from such Breach, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of University personnel responding to Breach, civil or criminal penalties levied against the University, attorney’s fees, court costs, etc. Any Breach may be grounds for immediate termination of this Agreement by the University.

VI. EXAMINATION OF RECORDS
University shall have reasonable access to and the right to examine any pertinent books, documents, papers, and records, regardless of the records’ format, of Contractor involving transactions and work related to this agreement until the expiration of five years after final payment hereunder. Contractor shall retain project records for a period of five years from the date of final payment.

VII. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS
Contractor shall make itself and any employees, subcontractors, or agents assisting Contractor in the performance of its obligations under the Agreement available to University at no cost to University to testify as witnesses in the event of an unauthorized disclosure caused by Contractor that results in litigation or administrative proceedings against University, its directors, officers, agents or employees based upon a claimed violation of laws relating to security, privacy or arising out of this agreement.
VIII. **SURVIVAL**
Contractor shall maintain an industry standard disaster recovery program to reduce in potential effect of outages because of supporting data center outages. Any backup site used to store university Protected or Private data will include the same information security and privacy controls as the primary data center(s).

In the event of termination of the Contract, for any reason, sections V, VI, and VII shall survive for a minimum of five years from the date of such termination.

IX. **RIGHT TO AUDIT**
Contractor agrees that, as required by applicable state and federal law, auditors from state, federal, Florida State University, or other agencies so designated by the State or University, shall have the option to audit the outsourced service. Records pertaining to the service shall be made available to auditors and the University during normal working hours for this purpose.