INFORMATION RISK MANAGEMENT PROGRAM

Unit Privacy Coordinator (UPC) Tasks

Information Security & Privacy Office

November 15, 2018

Version 1.8
The Unit Privacy Coordinator (UPC) manages a unit’s privacy program to meet university policy objectives.

The dean, director, or department head assigns the UPC role. The person, or persons, designated with the UPC role do not need to have a technical background. Administrative staff, data owners, Principal Investigators, 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.

**Policy Defined Tasks Include:**

1. **Maintain the information identification and classification documentation** of unit protected and private information assets.

2. **Assess the unit’s electronic and physical controls** for protected or private information to ensure they meet requirements.

3. **Ensure unit staff are trained** on the Information Privacy Policy, and specific legislated or contracted privacy requirements.

4. Ensure all unit personnel, e.g., faculty, staff, and students who handle protected or private information **sign a Florida State Employee Memorandum of Understanding** (or Legacy -Employee Statement of Understanding Regarding Confidentiality).

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 collected, processed, transmitted, or stored by a third-party vendor.**
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. Units must inventory and classify information, within their unit, to execute the assessment process in UPC Task 2.

**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. (Available by Request)

C. **What is a Dataset?** – Examples of datasets used to conduct university business.
2. Assess the unit’s electronic and physical controls for protected or private information to ensure they meet requirements.

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 and mitigate any control gaps.

**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. Its.fsu.edu>ISPO>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 should work with management, data owners, and systems administrators to identify and train individuals handling protected or private information. 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. ISPO has a training coordinator available to assist the UPC in setting up a training program.

**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. Its.fsu.edu>ISPO>Support Resources (links to select privacy legislation and contractual information including HIPAA, FERPA, GLBA, Human Subject Research)  
J. ISPO Training Coordinator
4. Ensure all unit personnel, e.g., faculty, staff, and students who handle protected or private information sign a Florida State Employee Memorandum of Understanding (or Legacy Employee Statement of Understanding Regarding Confidentiality).

The current Human Resources onboarding process includes the requirement of an employee to sign a Memorandum of Understanding. Legacy employees, hired prior to 2018, should have either a Confidentiality Statement on file or require the employee to sign the FSU Memorandum of Understanding form. The UPC will verify each employee handling “Protected” information has one of these documents on file.

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. Florida State Employee Memorandum of Understanding
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 collected, processed, transmitted, or stored by a third-party vendor.

Outsourced Service Involving the Transfer of Protected Information to a Vendor or the Collection of Protected Information by a Vendor as part of a Contracted Service

Payment is processed by Procurement Services

NO

Payment is not processed by Procurement Services or is purchased by PCard

YES

Vendor edits/redlines IT Security Terms and Conditions

NO

IT Security and Privacy Terms and Conditions are attached to Purchase Order (P.O.) terms and vendor accepts P.O. Terms

YES

ISPO will review edits and negotiate changes with Vendor

Vendor is processing information transmitted to or from the EU/UK or data sets designated as GDPR protected

NO

Vendor manually completes GDPR section of IT Security and Privacy Terms and Conditions

NO

P.O. ready for payment processing

YES
Resources:

A. Contract Addendum for University Sharing of any Information Classified as Protected and Private with a 3rd Party Vendor or Service Provider

###Sample Page 1 of Contract Terms

Florida State University INFORMATION
SECURITY and PRIVACY
Standard Terms and Conditions

June 2018

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, federal, European law/rules/regulations restricting the use and disclosure of such information, including the current versions of:

1) Gramm-Leach-Bliley Act (GLB) (15 U.S.C. §§ 6801(b) and 6805(b)(2)) (Select Student Aid Data);
2) Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) (Select Student Record Data);
3) Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub.L. 104–191, 110 Stat. 1936a (Select Personal Health Information for university covered components or university holders of a Business Associates Agreement);
4) Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (Select Personal Health Information for university covered components or university holders of a Business Associates Agreement);
5) Payment Card Industry Data Security Standard (PCI DSS) (Select Credit Card Data);
6) International Traffic in Arms Regulations (ITAR) (Select Research Data);
7) Export Administration Regulations (EAR) (Select Research Data);
8) Controlled Unclassified Information in Nonfederal Systems and Organizations NIST Special Publication 800-171;
9) Federal Trade Commission Red Flags Rule (Select Financial Data);
10) European General Data Protection Regulation (GDPR) (EU 2016/679) (Select Data Obtained by Persons in the European Union) (See Appendix A for further GDPR addendum requirements should GDPR protected information be identified and processed under the terms of the master agreement);