INFORMATION TECHNOLOGY SERVICES

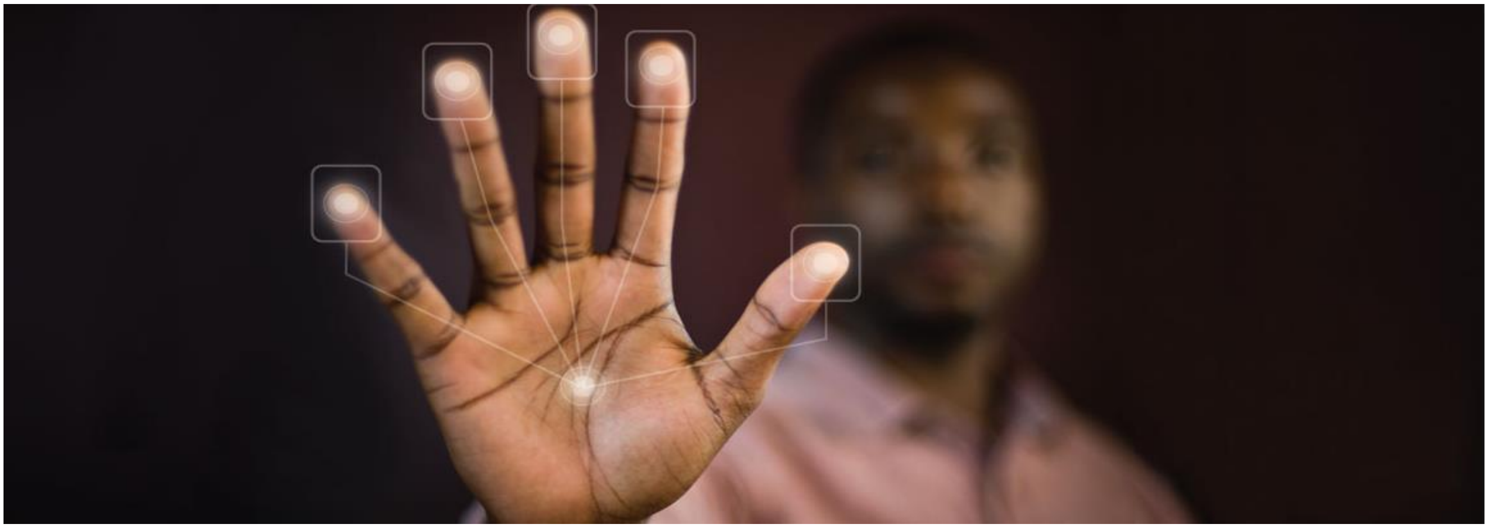
INFORMATION RISK MANAGEMENT PROGRAM

Unit Privacy Coordinator (UPC) Tasks

Information Security & Privacy Office

June 8, 2017

Version 1.5



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).

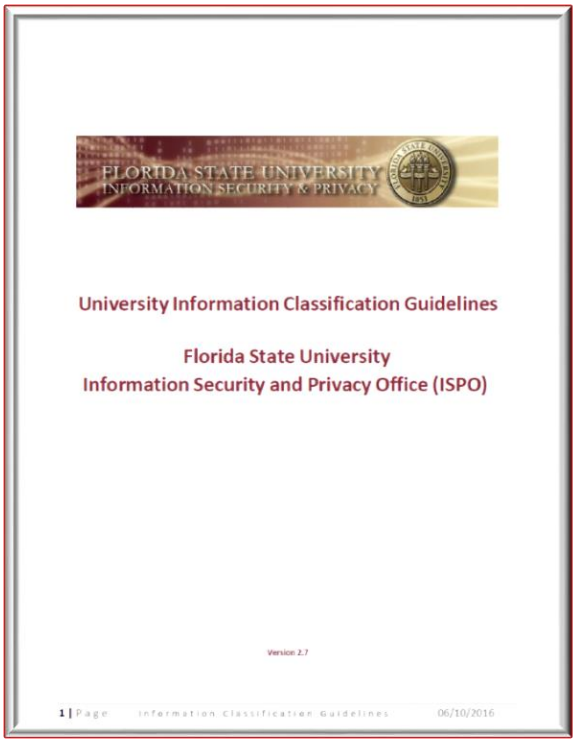
This document covers the basic functions of the UPC as outlined in the FSU Information Privacy Policy 4-OP-H-12.

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.



FLORIDA STATE UNIVERSITY
INFORMATION SECURITY & PRIVACY

University Information Classification Guidelines

Florida State University
Information Security and Privacy Office (ISPO)

Version 2.7

1 | Page Information Classification Guidelines 06/10/2016

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.

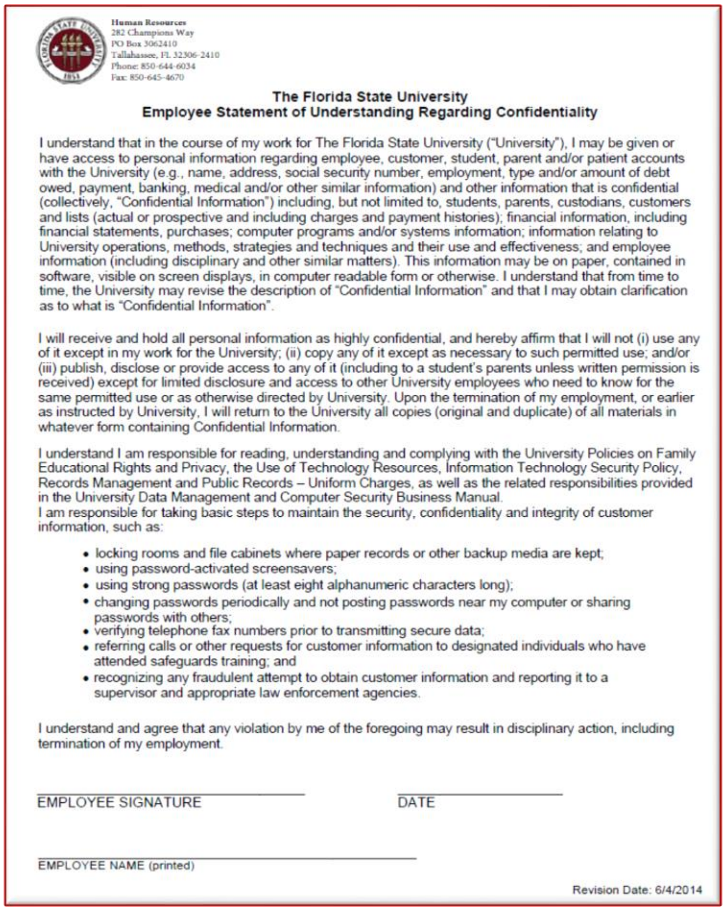
Resources:

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.



Human Resources
282 Champions Way
PO Box 3062410
Tallahassee, FL 32306-2410
Phone: 850-644-6034
Fax: 850-645-4670

The Florida State University
Employee Statement of Understanding Regarding Confidentiality

I understand that in the course of my work for The Florida State University ("University"), I may be given or have access to personal information regarding employee, customer, student, parent and/or patient accounts with the University (e.g., name, address, social security number, employment, type and/or amount of debt owed, payment, banking, medical and/or other similar information) and other information that is confidential (collectively, "Confidential Information") including, but not limited to, students, parents, custodians, customers and lists (actual or prospective and including charges and payment histories); financial information, including financial statements, purchases; computer programs and/or systems information; information relating to University operations, methods, strategies and techniques and their use and effectiveness; and employee information (including disciplinary and other similar matters). This information may be on paper, contained in software, visible on screen displays, in computer readable form or otherwise. I understand that from time to time, the University may revise the description of "Confidential Information" and that I may obtain clarification as to what is "Confidential Information".

I will receive and hold all personal information as highly confidential, and hereby affirm that I will not (i) use any of it except in my work for the University; (ii) copy any of it except as necessary to such permitted use; and/or (iii) publish, disclose or provide access to any of it (including to a student's parents unless written permission is received) except for limited disclosure and access to other University employees who need to know for the same permitted use or as otherwise directed by University. Upon the termination of my employment, or earlier as instructed by University, I will return to the University all copies (original and duplicate) of all materials in whatever form containing Confidential Information.

I understand I am responsible for reading, understanding and complying with the University Policies on Family Educational Rights and Privacy, the Use of Technology Resources, Information Technology Security Policy, Records Management and Public Records – Uniform Charges, as well as the related responsibilities provided in the University Data Management and Computer Security Business Manual.
I am responsible for taking basic steps to maintain the security, confidentiality and integrity of customer information, such as:

- locking rooms and file cabinets where paper records or other backup media are kept;
- using password-activated screensavers;
- using strong passwords (at least eight alphanumeric characters long);
- changing passwords periodically and not posting passwords near my computer or sharing passwords with others;
- verifying telephone fax numbers prior to transmitting secure data;
- referring calls or other requests for customer information to designated individuals who have attended safeguards training; and
- recognizing any fraudulent attempt to obtain customer information and reporting it to a supervisor and appropriate law enforcement agencies.

I understand and agree that any violation by me of the foregoing may result in disciplinary action, including termination of my employment.

EMPLOYEE SIGNATURE DATE

EMPLOYEE NAME (printed)

Revision Date: 6/4/2014

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.

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 should attach the university's IT security and privacy addendum and incorporate its provisions by reference. 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. Purchase orders and contracts to vendors that require the transfer of protected information that do not include the FSU security and privacy addendum are in violation of the FSU Information Privacy Policy.

Resources:

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