UNIVERSITY OF FLORIDA

INFORMATION PRIVACY
POLICIES & PROCEDURES
2012

GENERAL PRIVACY MANAGEMENT

UF | UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

Table of Contents

Rev: 02/01/2012

- **Mission and Scope of the Privacy Office** 4
  - Mission and Responsibilities
  - Scope of Regulations and Standards:
    - Federal, State, International, Industry
  - *Organizational Chart* 7
- **Privacy Personnel Designations** 8
  - Chief Privacy Officer
  - Privacy Office Staff
- **Policies, Procedures and Document Maintenance** 12
- **Privacy of University of Florida Identification Numbers – UFIDs** 14
  - UFIDs: Purpose and Use
  - Use and Protection of Student UFIDs
  - Privacy Requirements
- **Security of Restricted Information: General Privacy Safeguards** 16
  - Physical Safeguards: Securing Paper and Electronic Records
  - Administrative Safeguards 17
    - Policies and Procedures
    - Incident Management
    - Notice of Termination
  - Technical Safeguards 17
    - Access Controls
    - Password Controls
    - Account Management
- **Storage, Retention, Archiving and Disposal of Restricted Information** 19
  - Record Authority and Record Custodians
  - Arranging for Storage/Archiving 21
  - Requesting Approval for Record Destruction 22
  - Destroying Primary Records
  - *Record Destruction Methods Chart* 23
- **Identity Theft Prevention Program** 24
  - Privacy Requirements: Social Security Numbers 26
  - Financial and Consumer Information (Red Flags) 28
  - Security of Restricted Information 29
    - *Sample Form: Request to Use, Collect, or Store Social Security Numbers* 31
    - *Chart: Red Flag Indicators* 32

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Table of Contents (continued)

- Investigating and Responding to Privacy Violations 34
  - Policies
  - Definitions 36
  - Procedures: Investigation of a Complaint or Incident 38
  - Procedures: Response to Investigation 39
  - Procedures: Notification and Mitigation 41
    - *Flowchart: Responding to Privacy Violations* 44
    - *Flowchart: Notification Process* 45
    - *Matrix: Recommended Sanctions - Faculty & Staff* 46
    - *Matrix: Recommended Sanctions - Students* 47
    - *Article from Federal Trade Commission's Website* 48
    - *Sample Form: Investigation Summary* 50

NOTICE

The policies listed above and represented in the following pages apply to the University of Florida in all its campuses and locations.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Mission and Scope of the Privacy Office

❑ **POLICY** Rev: 05/01/2011

1. ***The mission of the Privacy Office*** is to ensure institutional compliance with federal and state privacy regulations, as well as industry standards, for restricted information; and to provide centralized resources, oversight and enforcement for privacy-related activities.

2. ***Responsibilities include***, but are not limited to:
   a. To develop, implement, and maintain University privacy-focused policies, procedures and guidelines that comply with statutory mandates and industry regulations.
   b. To deliver privacy-related training and to oversee privacy program monitoring and enforcement as required by privacy statutes and standards.
   c. To serve as the central contact and investigation authority for privacy complaints, incidents, and breaches. To coordinate the privacy notifications when required.
   d. To evaluate opportunities to reduce privacy risks and to execute program modifications that advance overall privacy compliance.
   e. To coordinate University medical records management and to provide consultation as University clinics transition to electronic medical record systems.

❑ **PRIVACY DEFINITIONS**

Restricted Information: Any and all personal identification information, protected health information, financial information, and other information protected by law or contract, applicable to the University of Florida or its affiliated entities, as the case may be, or their respective personnel in their official capacities, in any format (paper, electronic, or other). Examples include: medical records and medical record numbers; student UFID numbers, grades, schedules, records, and reports; selected human resource data; social security numbers; and any individual consumer financial account information, including credit and debit card numbers.
(See also: http://www.it.ufl.edu/policies/security/uf-it-sec-data.html)

❑ **THE SCOPE OF PRIVACY REGULATION AT UF**

1. ***Federal Statutes***
   a. Communications-related Statutes
      1) Children's Online Privacy Protection Act (COPPA)
      2) Cable Communications Policy Act
      3) Electronic Communications Privacy Act
   b. Family Education Rights and Protection Act (FERPA)
   c. Federal Privacy Act of 1974
   d. Individual Consumer Finance-related Statutes
      1) Fair Credit Reporting Act (FCRA)
      2) Financial Services Regulatory Relief Act of 2006

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Mission and Scope of the Privacy Office (continued)

3) Graham-Leach-Bliley Act (GLBA)
4) Right to Financial Privacy Act

e. Health-related Statutes:
1) Americans with Disabilities Act
2) Federal Substance Abuse Record Confidentiality
3) Genetic Information Non-Discrimination Act (GINA)
4) Health Insurance Portability & Accountability Act (HIPAA) for University and Affiliated Covered Entities / medical components; Faculty Practice Plans (e.g. UFP, UFJP/JHI, etc.); Health Science Center Colleges (Dentistry, Medicine, Nursing, Pharmacy, Public Health & Health Professions, Veterinary Medicine); Institute for Food & Agricultural Sciences (Dietetics); Student Health Care Center; Institutional Review Boards, Benefit and Disability Plans, and the UF Foundation
a) Organized Health Care Arrangement: Shands' Health Care System
b) Veterans' Administration Medical Center
c) Business Associates

f. Patriot Act

g. Proposed FTC Privacy Framework

2. Florida State Statutes

a. Chapter 90: Evidence
b. Chapter 119: Public Records
c. Chapter 381.004: HIV Testing
d. Chapter 384: Sexually Transmissible Diseases
e. Chapter 385: Chronic Diseases (Cancer Registry)
f. Chapter 392: TB Control
g. Chapter 393: Developmental Disabilities
h. Chapter 394: Mental Health
i. Chapter 395: Hospitals
j. Chapter 397: Substance Abuse
k. Chapter 400: Nursing Homes, Hospices
l. Chapter 405: Medical Research
m. Chapter 440: Workers' Compensation
n. Chapter 456-468: Health Professions
o. Chapter 501: Consumer Protection
p. Chapter 817: Privacy Breach Notification
q. Chapter 1002-1006: Education Records

3. International Regulations

a. Canada: Personal Information Protection & Electronic Documents Act
b. Council of Europe Convention for the Protection of Human Rights and Fundamental Freedom; European Union Data Protection Directive, Articles 1-33
c. US Department of Commerce's Safe Harbor Privacy Principles
d. Additional regulations in Argentina, Australia, Hungary, Iceland, Ireland, Japan, the Netherlands, and elsewhere.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Mission and Scope of the Privacy Office (continued)

4. Industry Standards

Payment Credit Industry Data Security Standards (PCIDSS)

- **REFERENCES:**

Federal Laws and Regulations (see http://www.usa.gov/Topics/Reference_Shelf/Laws.shtml)

Florida Statutes: (See list at Scope, above. View at: http://www.leg.state.fl.us/Welcome/index)

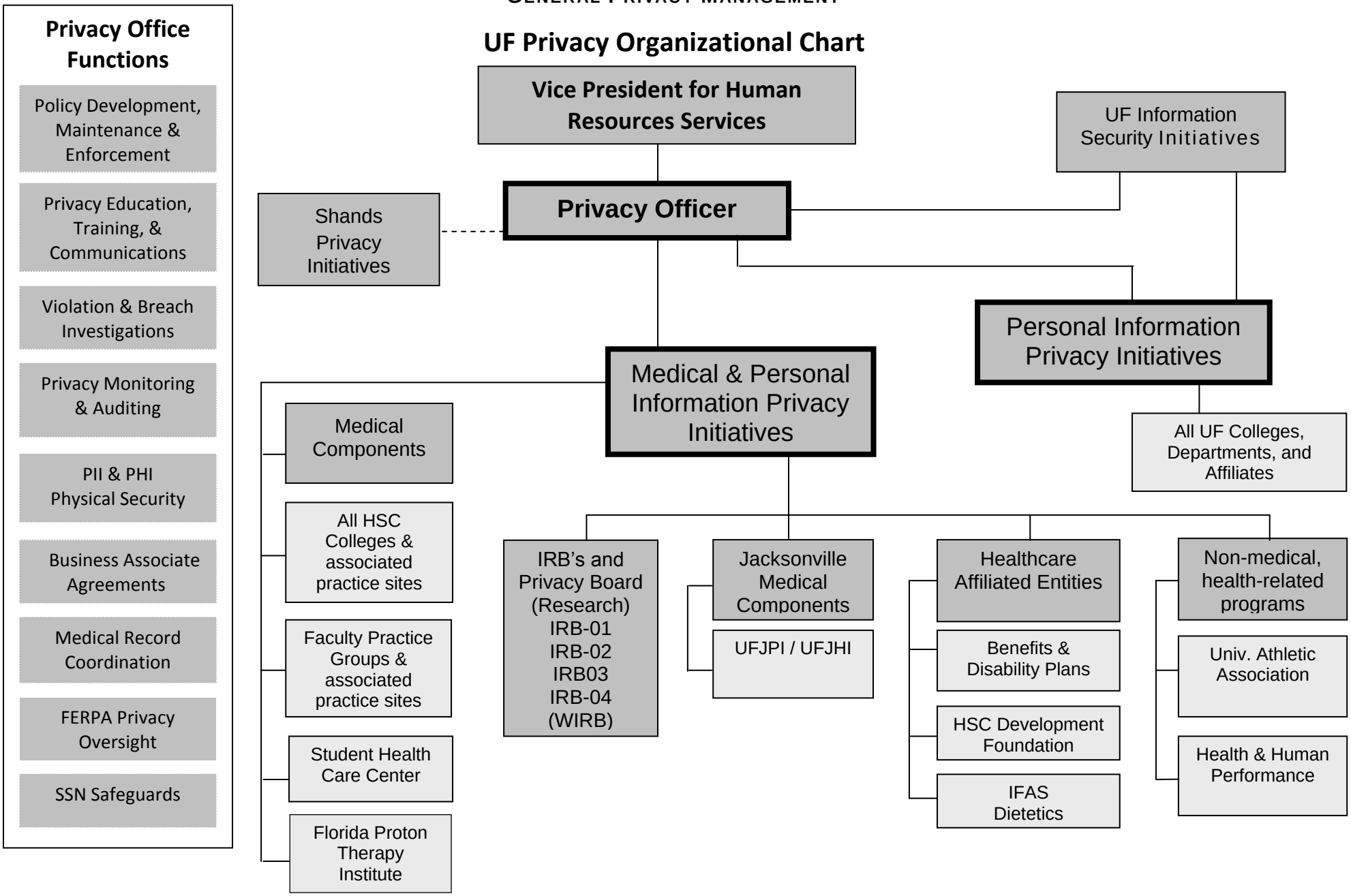
UF IT Data Security Standards: http://www.it.ufl.edu/policies/security/uf-it-sec-data.html

- **EXHIBITS:**

UF Privacy Organization Chart

© Copyright 2003 - 2008. University of Florida. All rights reserved.

UF Privacy Organizational Chart



© Copyright 2003 - 2008. University of Florida. All rights reserved.

Privacy Personnel Designations

- **POLICY** Rev: 02/01/2012

1. The University of Florida has designated a Chief Privacy Officer who is responsible for the development and implementation of the University's information privacy policies and procedures.
2. As University of Florida job descriptions are reviewed and revised, if job duties involve use and/or disclosure of restricted information, appropriate statements will be added to the job description to reflect this fact and the associated need for specialized training.

- **PRIVACY REQUIREMENTS**

1. Chief Privacy Officer

a. Purpose of Position: The Chief Privacy Officer is responsible for ensuring that the University of Florida, in its entirety, is compliant with international, federal and state privacy laws, especially HIPAA, FERPA, and SSN-related legislation.

b. Job Responsibilities
   1) Establishes, implements, manages, and coordinates all privacy-related activities at the University, including implementation and management of privacy-related policies and procedures. Assures University adherence and compliance with privacy regulations and organizational policies and procedures, investigates and mitigates privacy incidents, complaints, or breaches, and recommends disciplinary sanctions to University administration. Serves as information privacy consultant to the University for all departments and appropriate entities.
   2) Initiates, facilitates, and promotes activities to foster information privacy awareness. Oversees the design, development, and delivery of integrated privacy-security training. Tracks and reports mandatory privacy training compliance for general awareness, role-based, and research training programs.
   3) Oversees the implementation and coordination of HIPAA Administrative Simplification regulations for healthcare billing:
      a) The establishment of Business Associate Agreements for privacy and security relating to healthcare business associates.
      b) Privacy Board compliance with HIPAA-related research directives.
      c) University medical record management, including policies and procedures, and compliance with federal initiatives as well as federal and state medical records legislation.
   4) Regularly collaborates with key university stakeholders and affiliated entities about privacy-related issues. Maintains broad understanding of international, federal, and state privacy laws. Monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.
   5) Oversees all risk assessment and internal privacy audits to ensure regulatory compliance. Establishes audit plan and measures success.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Privacy Personnel Designations (continued)

6) Works with University administration, legal counsel, and other related parties to represent the university's information privacy interests with external parties. Cooperates with the Office of Civil Rights, other legal entities and university representatives in any compliance reviews or investigations.
7) Acts as privacy consultant to healthcare providers throughout Florida.

c. Qualifications:
1) Master's Degree in Health Administration, Business or other related field, or Law Degree required.
2) Experience in health information privacy and/or security with management responsibilities required.
3) Extensive familiarity with relevant health care legislation and standards for the protection of health information and patient privacy required.
4) Experience in a university or academic medical center preferred.
5) Extensive knowledge of legal and regulatory issues as they relate to higher education and healthcare required. An understanding of network and system security, especially as it relates to the health information environment required.
6) Ability to work effectively in a collegial, consensus-driven organization required.
7) Excellent verbal and written communication skills, as well as interpersonal skills required. Must be able to problem-solve, prioritize assignments and effectively manage projects.

2. Privacy Manager, UF Jacksonville

a. Purpose of the Position: Responsible for all designated UF Privacy operations on the Jacksonville Health Science Center Campus.

b. Job Responsibilities
1) Assist Chief Privacy Officer with investigation of privacy incidents and complaints, implementation of policies and procedures, and coordination of privacy education on the UF Jacksonville campus.
2) Maintain the documentation for privacy incident investigations, resolutions, and sanctions.

c. Qualifications
1) Master's Degree preferred or Bachelor's Degree and six years experience.
2) Minimum two years experience in health care environment.
3) Certified Information Privacy Professional required.

3. Privacy Manager / Coordinator, HIM and Training

a. Purpose of the Position: Works with the Chief Privacy Officer to interpret federal and state privacy laws and regulations for the development of privacy policies and procedures that will ensure compliance with both legal requirements and professional standards; monitors daily health information activities for the confidential and secure management of health information created, received, and maintained by the University of Florida; provides privacy-related education and training materials for use by faculty, staff, students, and volunteers.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Privacy Personnel Designations (continued)

b. Job Responsibilities
   1) Incorporate new privacy-related federal and state legislative requirements into UF privacy policies and procedures by timely updating and amending UF privacy policies and procedures.
   2) Serve as the Honest Broker Services Coordinator for the University of Florida to collect and provide de-identified health information to research investigators.
   3) Act as a resource on Health Information Management throughout the organization and as a liaison among the University's health information users and delegated custodians, the Shands HealthCare Health Information Management departments, and other internal/external stakeholders.
   4) Formulate, present, document, and report the educational activities required by federal and state privacy regulations, as needed.

c. Qualifications
   1) Master's Degree or Bachelor's Degree and two years appropriate experience.
   2) Registered Health Information Administrator
   3) Certified Professional Trainer or previous experience with adult professional education strongly desired.

4. Privacy Analyst

a. Purpose of the Position: To investigate reported incidents and complaints related to state and federal privacy laws, and University of Florida policies and procedures regarding the privacy of health and personal information.

b. Job Responsibilities
   1) Serve as delegated Privacy Breach Notification Coordinator.
   2) Assist Chief Privacy Officer with investigation of privacy incidents and complaints.
   3) Maintain the documentation for privacy incident investigations, resolutions, and sanctions.

c. Qualifications
   1) Master's Degree or Bachelor's Degree and two years experience.
   2) Minimum two years experience in health care environment.
   3) Certified HIPAA Professional preferred.

5. Privacy Auditor

a. Purpose of the Position: To audit compliance with state and federal privacy laws, as well as University of Florida policies and procedures regarding the privacy of health and personal information.

b. Job Responsibilities
   1) Assist with the design and implementation of the audit strategic plan for the Privacy Office.
   2) Formulate, conduct, document, and report on auditing activities related to the privacy regulations, including, but not limited to:
      a) Identifying and assessing privacy risks
      b) Planning and conducting operational privacy-related audits
      c) Compiling audit work-papers and reporting findings and recommendations

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Privacy Personnel Designations (continued)

3) Maintain liaison with UF colleges and departments, UF Information Technology groups, and Shands HealthCare system to coordinate and complete investigative reviews.

c. Qualifications
   1) Master's Degree or Bachelor's Degree and two years experience.
   2) Minimum two years experience in health care environment.
   3) Certified Internal Auditor preferred.

- **REFERENCES**

  HIPAA Regulations: 45 CFR § 164.530(a) (Personnel Designations), §164.308(a)(2) (Assigned Security Responsibility)

- **EXHIBITS** None

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Policies, Procedures and Document Maintenance

❑ **POLICY:** Rev: 05/01/2011

1. The University of Florida has developed policies and procedures with respect to restricted information that comply with federal and state regulations. The Chief Privacy Officer is responsible for developing, maintaining, revising, and enforcing all privacy policies and procedures.
2. The University of Florida will revise policies and procedures as needed to maintain compliance with changes in the law. Policies and procedures are also reviewed at least annually, and revised as needed.
3. Any changes in privacy practices or in privacy policies and procedures are documented and published on the Privacy Office web site as soon as possible; reasonable efforts are made to communicate the changes to individuals who may be affected by them. The revision date of policies and procedures appears on each document.
4. The University of Florida reserves the right to change its policies and procedures at any time, and to make such changes effective for restricted information that it has created or received prior to the effective date of the revision.
5. Policies and procedures are maintained by the Privacy Office in written form, which may be printed and/or electronic formats. Copies are available on the University of Florida Privacy Office web site. Paper copies may be obtained from the Privacy Office during normal business hours.
6. Any communication, action, activity, or designation that is required by federal or state privacy regulations to be documented or in writing (i.e., training records, complaint investigations, privacy audits, accounting logs, etc.) will be maintained by the responsible college, department, or unit in writing, (which may be printed and/or electronic formats) for at least six years from the date of creation or the last effective date, whichever is later.

❑ **DEFINITIONS**

Documentation: evidence or substantiation that certain actions were completed, information was collected, used or disclosed, or requirements were met.

Policy: An overall plan defining goals and objectives.

Procedure: A series of steps or processes used to achieve stated goals; a set of formalized instructions.

❑ **PROCEDURES**

The following policies and procedures will be maintained to comply with federal and state privacy laws and regulations or University Regulations for all Restricted Information:

1. Privacy Office Mission and Scope
   a. Mission Statement

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Policies, Procedures and Document Maintenance (continued)

b. Laws, Statutes, Regulations

2. Privacy Personnel Designations
   a. Chief Privacy Officer
   b. Privacy Training Coordinator
   c. Privacy Auditor
   d. Privacy Analyst
3. Policies, Procedures and Document Maintenance
   Inventory of Policies and Procedures
4. Security Safeguards: Electronic Records
   a. Administrative Safeguards
   b. Physical Safeguards
   c. Technical Safeguards
5. Privacy of University of Florida Identification Numbers – UFIDs
6. Identity Theft Prevention Program
   Use of Social Security Numbers and Financial Information
7. Record Management Procedures
   a. Storage, Retention and Archiving
   b. Disposal and Destruction
8. Reporting, Investigating and Responding to Privacy Violations
   a. Reporting Privacy Incidents
   b. Refraining from intimidating or retaliatory acts
   c. Investigation Process: Complaints / Incidents
   d. Actions When No Violation is Found
   e. Actions When a Violation is Found
   f. Corrective Actions and Sanctions
   g. Mitigation
   h. Notification

❑ **REFERENCES:**

45 CFR §164.530(i) & (j) and §164.316(a) & (b) (Policies and Procedures and Documentation)

❑ **EXHIBITS:** None

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Privacy of University of Florida Identification Numbers (UFIDs)

❑ **POLICY:** Rev: 02/01/2012

1. ***University of Florida Identification Numbers (UFIDs)*** are the property of the University of Florida; use and governance of such numbers shall be at the discretion of the University, within the parameters of the law. See the history and policies for UFIDs: http://www.it.ufl.edu/ufid/, http://www.bridges.ufl.edu/faqs/UFID.shtml.

2. ***Student UFIDs are classified as restricted data*** by the University of Florida and are considered part of the student's "Educational Record", as defined by FERPA, when the number can "be used to gain access to education records," i.e., "when used in conjunction with one or more factors that authenticate the user's identity, such as a personal identification number (PIN), password or other factor known or possessed only by the authorized user." (T34-§ 99.3 - Directory Information(c)(1))
   a. Student UFIDs, in whole or in part, may not be used as identifiers to publicly post or display grades or other personal student information.
   b. Student UFIDs may be included in E-mail communications under specific conditions and for limited purposes, as follows:
      1) UFIDs may only be used in e-mails related to official University records and only to perform authorized business transactions where unique identification of students is necessary.
      2) Internal e-mail communications containing student UFIDs may only be sent from one *ufl.edu* address to another *ufl.edu* address.
         a) The sender of an e-mail containing student UFIDs is responsible for ensuring that the recipient's address is within the *ufl.edu* e-mail system.
         b) E-mail containing student UFIDs may not be manually forwarded or auto-forwarded to any non-*ufl.edu* account, including, but not limited to, personal and commercial e-mail accounts such as AOL, Yahoo, MSN, G-Mail, etc.
         c) A student UFID may not be included with the student's name in the subject line of e-mails. Limited student names with associated UFIDs may be included in the body of the email.
         d) Lists of student UFIDs (more than 3) should not be included in the body of emails, but instead should be included in an electronically secured (at least password protected) attachment.
      3) Authorized external e-mail communications (sent outside the *ufl.edu* domain) that include student UFIDs must be protected by encryption.
      4) No distribution list, whether departmental or personal, may be used for e-mail that includes student UFIDs.
      5) Access to *ufl.edu* e-mail accounts through the Internet must be by secure (SSL) connections.
   c. *E-Mail Scope:* This policy applies to all use of electronic mail systems within the University of Florida where the mail originated from or is forwarded into a University of Florida computer or network. It applies to all e-mail users including, but not limited to, faculty, staff, students, and volunteers.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Privacy of University of Florida Identification Numbers (UFIDs) (continued)

3. ***Employees, volunteers, and students may be subject to disciplinary action***, up to and including termination of employment or dismissal from the University for violating this policy and/or breaching the confidentiality of UFID's. Any such disciplinary action shall be governed by the regular University policies and procedures applicable to the situation.

❑ **DEFINITIONS**

UFID: Implemented on January 21, 2003, the UFID is an identifier for all University of Florida faculty, staff and students. The UFID is an eight-digit number displayed using a dash between the fourth and fifth digits as in *1234-5678*

E-mail: A means or system for transmitting written messages electronically (as between terminals linked by telephone lines, cable networks, or microwave relays).

❑ **PRIVACY REQUIREMENTS**

The University of Florida is required to implement appropriate administrative, technical, and physical safeguards to maintain the privacy and security of restricted information.

❑ **PROCEDURES**

1. ***Encryption may be accomplished in either of the following ways:***
   a. Encrypt the connection(s) between sender and receiver (i.e through SSL, TLS or VPN), or
   b. Place the UFIDs in a word or data file, protect the file using a strong pass code, and communicate the pass code to the recipient in a secure fashion. DO NOT include the pass code in the email with the file.
2. ***Include the following confidentiality statement*** or a comparable statement in all e-mails that are sent from the University of Florida:
   NOTE: This communication may contain information that is legally protected from unauthorized disclosure. If you are not the intended recipient, please note that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, you should notify the sender immediately by telephone or by return email and delete this message from your computer.

❑ **REFERENCES**

Title 34: Education – Part 99: § 99.3
Florida Statutes: 817.568 Criminal use of personal identification information.
UF Policies: UF Information Technology Security Policies

❑ **EXHIBITS:** None

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Security of Restricted Information: General Privacy Safeguards

❑ POLICY

Rev. 05/01/2011

All restricted information in all formats should be secured from unauthorized access at all times, to protect the information from damage, loss, alteration, tampering, and fraudulent use.

❑ DEFINITIONS

Safeguards: Rules and specific methods established to protect restricted information from unauthorized access, accidental or intentional use, disclosure, transmission, or alteration, and inadvertent or incidental disclosure to unintended recipients.

❑ PRIVACY REQUIREMENTS

The University of Florida is required to implement appropriate administrative, technical, and physical safeguards to maintain the privacy and security of restricted information.

❑ PROCEDURES

1. Physical Safeguards for Restricted Information

a. Securing Paper Records

1) Place paper records in protective folders or binders that are clearly marked with a name and/or other identifier. Review the contents of the folder periodically to ascertain that it contains only information pertaining to that record.
2) Keep records and documents that are not currently in use in locations that can either be locked or that will be occupied by authorized personnel at all times. Double locking is preferred; i.e., a lockable storage unit inside a lockable room.
3) Records that are in use for operations purposes should be in the physical possession or view of an authorized workforce member at all times.
4) Shred discarded record documents immediately or place them in a secure storage area for controlled shredding later. Do not place papers containing restricted information in open waste receptacles. Collect papers for recycling only in designated secure locations.
5) Place computer printers and fax machines in locations that can either be locked or that will be occupied by authorized personnel at all times.

b. Securing Electronic Records

1) To prevent unauthorized use, place computers, monitors, laptop computers, and similar data storage and display devices in areas that limit or prevent access by unauthorized persons.
2) To prevent unauthorized viewing of restricted information, position electronic data devices away from public view or shield the monitor screen.
3) University personnel who access restricted information at home or in other non-work locations are also expected to use physical safeguards to prevent family members, roommates, and friends from unauthorized viewing of records.
4) Encrypt all restricted information stored on removable electronic storage media (discs, tapes, CD's, keys, etc.).

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Security of Restricted Information: General Privacy Safeguards (continued)

5) When no longer needed, physically destroy removable electronic storage media (discs, tapes, CD's, keys, etc.) that have been used for storing restricted information, or place in a locked storage unit for secure controlled destruction later.
6) Electronically purge data devices used to store restricted information before they are discarded or otherwise taken out of the control of the University.

2. Administrative Safeguards for Restricted Information

a. Policies and Procedures: Follow the policies and procedures for preventing, detecting, containing, and correcting security breaches and violations, as required by Unit Information Security Administrators and Managers.

b. Incident Management: Report security incidents involving inappropriate use or disclosure of restricted information to the Privacy Office immediately.
   1) Report known and suspected security incidents to the appropriate Unit Information Security Administrator and/or Manager for investigation, repair, restoration, and disciplinary action, as necessary.
   2) Security incidents include viruses, worms, hoax e-mails, hacking, altered data, deliberate disruptions of service, and other unauthorized use of computer accounts and systems.

c. Notice of Termination
   1) Supervisors must notify the Information Technology Department immediately when an employee terminates employment so that access to electronic data systems may be terminated.
   2) Supervisors are also required, when an employee terminates employment, to collect keys and other access devices if the employee's job duties included authorized access to any area where restricted information is stored or used.

3. Technical Safeguards for Restricted Information

a. Computer Access Controls: To prevent unauthorized use, program all electronic computing and data devices with log-on protocols and automatic screen-savers that are password protected.

b. Password Controls and Guidelines
   1) Construct and use "strong" passwords according to UF network rules. Change passwords at least every 90 to 120 days.
   2) Use different passwords for different accounts, both at work and at home.
   3) Do not write down, post, include in e-mail, or otherwise share passwords with anyone. If the security of a password is in doubt, change it immediately.
   4) Do not bypass password entries by auto-logons or "remember-me" applications.

c. Account Management: As accounts are the means to control access, verify the identity of users, and hold users accountable.
   1) Create accounts only for approved requests for access that are appropriate for the system or service.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Security of Restricted Information: General Privacy Safeguards (continued)

2) Assign uniquely identifiable accounts to authenticated users.
3) Routinely monitor accounts for use and activity.
4) Authorize only those capabilities within each account that are appropriate to the user's role requirements, responsibilities, and specific needs.

- **REFERENCES**

Florida Statutes: 817.568 Criminal use of personal identification information.
UF Policies: UF Acceptable Use Policy, UF Information Technology Security Policies

- **EXHIBITS:** None

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Storage, Retention, Archiving, and Disposal of Restricted Information

❑ **POLICIES** Rev. 05/11/2011

1. ***Authority:*** The University of Florida has implemented storage, retention, and disposal policies for records containing restricted information, based on standards of professional practice, risk management guidelines, and the retention schedules listed in the Florida Statutes and University Regulations. Chapter 119, Florida Statutes, Public Records Act, defines public records and establishes the legal basis for the custody and disposal of public records.

2. ***Record Custodians:*** University Regulations (4.007) allow the President of UF to delegate record custodian duties to the Vice Presidents: "(3) Each Vice President may designate an individual in his or her area as the custodian of records for that area."

   Each college and department that creates, receives, maintains, uses, and/or discloses personally identifiable and other restricted information in any format, should also designate at least one staff member to manage the information and records for that area.

   The staff member is not required to be solely dedicated to the management of information, but should be specifically trained and responsible for maintaining the confidentiality, security, and accessibility of restricted information.

3. ***Storage:*** All records that contain restricted information must be stored in physically secure areas that are protected from unauthorized access, damage by fire, water, insects, and other pests, and that are environmentally controlled for temperature and humidity.
   a. Records should be organized and stored to facilitate easy retrieval by authorized staff members.
   b. Department staff should not remove records without notifying the designated records manager.

4. ***Archiving:*** Restricted information in paper or electronic format, which is not being actively used may be archived until the retention requirements have been met.
   a. Colleges, departments, and other units determine the criteria for inactive record status in their areas, based on need for the records and available storage space.
   b. Only primary records should be archived. The contents of "Shadow" records should be destroyed after it has been determined that they contain only duplicates of records maintained elsewhere, and do not contain any original materials.
   c. Off-site storage facilities or organizations for back-up electronic records containing restricted information must be approved by the Privacy Office.

5. ***Record Destruction and Disposal:*** Primary records containing restricted information shall only be destroyed in the ordinary course of business; no entire record shall be destroyed on an individual basis.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Storage, Retention, Archiving, and Disposal (continued)

a. No primary records of any type belonging to the University of Florida may be destroyed until:
   1) The records have met established retention requirements, and
   2) A Records Disposition Request has been approved by the University Records Management Office.
b. No records that are pending or currently involved in investigations, audits, or litigation shall be destroyed or otherwise discarded.
c. Records containing restricted information should only be destroyed by a bonded and insured professional document destruction company.

❑ DEFINITIONS

Archiving / Storage: The act of physically moving inactive or other records to a storage location until the record retention requirements are met or until a record is needed for active use again.

Destruction of Records: The systematic permanent disposal of records that have been maintained for the prescribed retention period. The purpose of disposal or destruction is to permanently remove records from active use, with no possibility of reconstructing the information contained in them, while maintaining the confidentiality of any restricted information they may contain.

Disposal of Records: The day-to-day discarding of duplicate or extra reports that are not pertinent to business needs.

Inactive Records: Official University, college, department, or other unit records that have not been actively added to, billed for, or involved in litigation or research for a designated period of time.

Primary Record: Original documentation created and collected by University employees in the regular course of their duties in carrying out the mission of the University. They are usually maintained in and/or by the entity where the information was collected or the services were provided and are considered the legal documents business purposes.

Scheduling Records: Identifying the types of records and then determining how long a particular type of record must be retained, according to the UF General Records Schedule.

Shadow Record: A record containing original documentation that is temporarily, for whatever reason, kept apart from the primary record. It may also contain copies and/or other materials that employees desire to save, but are not needed in the primary record (material to be purged); however, the original documents will eventually be included in the primary record.

❑ PRIVACY AND STATUTORY REQUIREMENTS

1. ***Retention of Records:*** A "schedule" describing the records and the official retention period is required by the state of Florida for each type of record created or maintained by public institutions.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Storage, Retention, Archiving, and Disposal (continued)

a. Chapter 257, Florida Statutes, establishes the State's Records Management and Archives Program under the direction of the Division of Library and Information Services, Department of State, as well as specifically provides for a system for the scheduling and disposal of public records.

b. Record Schedules: The University uses several different schedules, including:
   1) General Records Schedule for State and Local Government Agencies (GS1-S and GS1-L),
   2) General Records Schedule for Universities and Community Colleges (GS-5),
   3) General Records Schedule for Public Health Care Facilities and Providers (GS-4), and
   4) Individual records schedules developed specifically for the University of Florida. (See the UF General Records Schedule in Appendix B).

2. ***Obtaining Disposition Authorization:*** When records have met retention requirements established by the UF General Records Schedule, disposal action may be initiated by submitting a Records Disposition Request to the UF Records Management Office.
   a. The UF Records Manager will forward the request to the Office of General Counsel and the University Archives.
   b. If approved, the request form authorizes the disposition of the listed records, and serves as documentation of records destroyed. The request must be submitted and approved before actual disposition is carried out.

❑ **PROCEDURES**

1. ***Arranging for Storage of Inactive or Back-Up Records****:* Approved storage areas for records containing *Restricted Information* include:
   a. On-Site: An area inside the college, department, or other university facility that meets the criteria listed above. Record owners are responsible for making arrangements to move the records.
   b. Off-Site: A professional record storage company with which the University of Florida has an active contract for services.
      1) Call the Privacy Office or UF Purchasing for information about currently contracted storage facilities. Transport of records is included in services. Inventorying of records may also be arranged on the request of the record owner.
      2) Other arrangements for complying with security policies requiring off-site storage of back-up electronic media should be proposed in writing for approval by the Privacy Office.

NOTE: These are NOT acceptable for storage of <u>inactive</u> records containing restricted information: Moving and storage warehouses, mini-storage facilities, and off-campus personal or rental property of staff members, including garages, homes, mobile homes, trailer, etc.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Storage, Retention, Archiving, and Disposal (continued)

2. ***Archiving Inactive Records:***
   a. Place records in storage boxes in an orderly manner to facilitate retrieval, if needed. Label each container with a clear description of the contents, the date-range, and the college, department or other unit from which the contents came.
   b. Maintain an inventory of the boxes so that records can be found, if necessary. If records are retrieved from storage, track the status (active or inactive) and adjust the inventory as needed.
   c. **Shadow** Records: Purge shadow records often and in reasonable batches to avoid overwhelming filing areas (where the primary records are stored) with large amounts of documentation to be filed.
      1) Review the contents of "shadow" or duplicate records and remove any original materials. Send original documents to be filed in the primary record. Do not send entire shadow charts to the record custodian for inclusion in the primary record.
      2) Follow the protocols for record disposal to permanently destroy the duplicate parts of the record.
   d. Place the records in storage using the **storage facility's guidelines**, if appropriate.

3. ***Requesting Approval for Record Destruction***
   a. Complete the UF Records Disposition Request prior to commencing any record destruction procedures. Follow the instructions included with the form.
   b. Send the Request to the UF Records Manager at the address on the form. Authorization to destroy records may take 6 to 8 weeks to process.

4. ***Disposing of Non-Primary Records Containing Restricted Information*** (i.e., duplicate, extra, or obsolete individual reports or data)
   a. <u>Destruction:</u> Paper records and records stored on electronic media must be either immediately shredded, pulverized, or electronically purged, or placed in locked or otherwise secure storage for controlled shredding/destruction and recycling later. See the table at the end of this chapter.
   b. <u>Recycling:</u> Papers containing restricted information may be placed in secure recycling bins provided by a contracted document destruction company. Papers that have been shredded should not be placed in these recycling bins, but may be placed in generic recycling containers for pickup by UF's Physical Plant Department.

5. ***Destroying Primary Records Containing Restricted Information***
   a. Maintain records that are scheduled for destruction in a secure location to guard against unauthorized or inappropriate access.
   b. Follow the record destruction company's protocol for carrying out the actual destruction.
   c. Sign the completed UF Records Disposition Request after the destruction has been completed.
   d. Attach the Certificate of Destruction provided by the record destruction company to the UF Records Disposition Request.
   e. Maintain all documentation of record destruction for the life of the institution.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Storage, Retention, Archiving, and Disposal (continued)

- **REFERENCES:**

  Florida Statues: Ch 119.01 (General policy on public records), Ch 119.011 (Definitions), Ch 119.021 (Custodial requirements, maintenance, preservation, and retention of public records), Chapter 257.36 (5) and (6) (Records and information management)

- **EXHIBITS:** Chart: Appropriate Record Destruction Methods

Appropriate Record Destruction Methods	
Medium	**Recommendation**
Paper Records	Shred (preferably cross-shred), pulp, burn, or pulverize
Audiotapes & Videotapes	Recycle by recording over by the original user, or pulverize the tape and cassette
Computerized Data / Hard Disk Drives / Magnetic Media / Memory Sticks, Keys and other memory devices	Professionally purge (degauss) by a certified, licensed, and bonded vendor and pulverize
Computer Diskettes	Reformat and over-write all data, pulverize, or magnetically degauss
Laser Disks / Compact Disks	Shred or pulverize in appropriate equipment, OR break, using layers of newspaper and a hammer, OR thoroughly scratch both sides with knife or key
Microfilm / Microfiche	Shred or pulverize only

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Identity Theft Prevention Program

Use of Social Security Numbers and Financial Information

❑ **POLICIES** Rev. 02/01/2012

1. The University will make every reasonable attempt to protect the personal identification and personally identifiable financial information it creates, receives, maintains, and transmits, and to comply with current laws that provide for the protection of these types of information.
2. As allowed and/or required by law, the University of Florida will collect, maintain, use, and disclose Social Security Numbers and credit card or other financial information of employees, students, clients, patients, vendors, and others in the ordinary course of its business.
3. Each University entity with access to personal identification or personally identifiable financial information is responsible for developing and implementing procedures to comply with the Identity Theft Prevention Program.

❑ **DEFINITIONS**

Account means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

- An extension of credit, such as the purchase of property or services involving a deferred payment; and
- A deposit account.

Covered Account means:

- An account that the University of Florida offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, student account, or other financial accounts; and
- Any other account that the University offers or maintains for which there is a reasonably foreseeable risk to Customers (Consumers) or to the safety and soundness of the institution from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Credit means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

Credit Card Information includes:

- Credit card number (in part or whole) with or without its verification number
- Credit card expiration date
- Cardholder name
- Cardholder address

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Identity Theft Prevention Program (continued)

Creditor: ''(A) means a creditor, as defined in section 702 of the Equal Credit Opportunity Act (15 U.S.C. 1691a), that regularly and in the ordinary course of business—

''(i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;

''(ii) furnishes information to consumer reporting agencies, as described in section 623, in connection with a credit transaction; or

''(iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person (*i.e., financial aid or Gator1 debit cards)*;

''(B) does not include a creditor described in subparagraph (A)(iii) that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person *(i.e., lawyers, doctors, accountants, dentists, orthodontists, pharmacists, veterinarians, nurse practitioners and social workers and other service providers*); and

''(C) includes any other type of creditor, as defined in that section 702, as the agency described in paragraph (1) having authority over that creditor may determine appropriate by rule promulgated by that agency, based on a determination that such creditor offers or maintains accounts that are subject to a reasonably foreseeable risk of identity theft.''.

Customer (Consumer) means a person that has a Covered Account with the University of Florida.

Identity Theft (16 CFR 603.2(a)) means a fraud committed or attempted using the identifying information of another person without authority. The term "identifying information" refers to any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any--

- Name, Social Security Number, date of birth, official state or government issued driver license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code; or
- Telecommunication identifying information or access device.

Records: Any document, file, database, image, recording, or other means of expressing fixed information, made or received by an institution according to law or its particular mandate and preserved by it in any form as evidence or information.

Record Systems: All mechanisms and media used for input, storage, organization, display, retrieval, and printing of records. Systems consist of components including, without limitation, computers, computer peripherals, wired and wireless networks used for voice and data, as well as fax machines, photo copiers or paper, and paper filing systems.

Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Identity Theft Prevention Program (continued)

Social Security Number: A unique nine-digit number assigned to individuals in the United States of America for the purpose of administering the Social Security laws. Truncated forms (last four digits, first three digits, etc.) of the number are also considered restricted data.

Telecommunication access device means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument). (18 U.S.C. 1029(e))

Telecommunication identifying information means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument. (18 U.S.C. 1029(e))

Workforce means all faculty, staff, students and volunteers, temporary and permanent, full-time and part-time, with access to personal identification and financial information who are employed by or otherwise associated with the University of Florida and their affiliated entities.

- **PRIVACY REQUIREMENTS**

1. ***Social Security Numbers***
   a. *Classification:* Social Security Numbers obtained by the University are classified as restricted data and must be protected from unauthorized use or disclosure.
      1) Security protocols, including those for any hardware and software housing restricted data, will be subject to audit by the University's internal audit office and information technology offices.
      2) In limited circumstances, with documented approval from the Chief Privacy Officer, individuals and entities may be allowed to use Social Security Numbers or truncated (last four digits) Social Security Numbers for certain specific purposes.
   b. *Authorized Uses and Requests for Exemption:*
      1) Individuals and units with a bona fide need to collect Social Security Numbers beyond those that are already authorized (listed below) must request an exemption by memorandum through the Privacy Office. The exemption request must:
         a) State the intended use of the number,
         b) Describe in detail the physical and technical security protocols that will protect the data from compromise, and
         c) State how written notice of the use of the number will be provided to the owner.
      2) Authorized uses of Social Security Numbers include:

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Identity Theft Prevention Program (continued)

a) Tax Reporting – required as a taxpayer ID for all tax information reported to the IRS, including:
   i. Wage and withholding data for full-time and part-time employees,
   ii. Honoraria provided to guest lecturers,
   iii. Independent contractors working for the University,
   iv. Payments to research participants for 1099s.
b) Financial Aid – to obtain federal financial aid information and to identify and confirm the level of financial aid assistance.
c) Human Resource Services – approved for use on federal I-9 forms for hiring purposes, employment verification, and by certain benefit providers, such as insurance companies for verification of eligibility and coordination of benefits.
d) Law Enforcement – Federal and state agencies often rely upon SSN's as the primary identifier for law enforcement and criminal information purposes. In the event such agencies request SSN information using proper procedures, it will be provided following review and approval through the Privacy Office in consultation with the Office of the General Counsel.
e) Business Imperatives of the University:
   i. Identity Management – to maintain the integrity of student records and verify the identities of students and workforce members.
   ii. External Reporting – to fulfill the University's responsibility to provide transcripts and other information for which more universally known IDs are needed and approved.

c. *Collection of Social Security Numbers:*
   1) An entity of the University may not collect an individual's Social Security Number unless the entity has stated in writing the purpose for its collection and unless it is:
      a) Specifically authorized by law to do so; or
      b) Imperative for the performance of that entity's duties and responsibilities as prescribed by law.
   2) Social Security Numbers collected by an entity of the University may not be used by that entity for any purpose other than the purpose provided in the written statement.
   3) An entity of the University collecting an individual's Social Security Number shall provide that individual with a copy of the written statement required above.

d. *Training:* Workforce members, including students and volunteers, who have access to Social Security Numbers must complete Social Security Number Privacy Training during their initial orientation and annually, thereafter.
   1) Self-directed training modules are available on the Privacy Office website. Classroom instruction is available by request through the UF Privacy Office.
   2) Unit supervisors/unit administrators are responsible for implementing appropriate unit training requirements based on the job duties of workforce members in the unit.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Identity Theft Prevention Program (continued)

e. Responding to a Privacy Breach: Promptly report loss or theft of Social Security Numbers from University records or record systems to the Privacy Office for immediate investigation.

2. ***Financial and Consumer Information***: If a University organization is a Creditor and maintains Covered Accounts (see Definitions above), the organization must initiate and maintain Identity Theft Prevention Program procedures.
   a. Program Administration
      1) The Identity Theft Prevention Program is the responsibility of the University of Florida's Board of Trustees, which will approve the initial program, recertify the program annually, and maintain appropriate documentation of the program and its subsequent amendments.
      2) Operational responsibility of the program is delegated to the University's Privacy Office.
   b. Identifying Red Flags: A Red Flag, or any situation closely resembling a Red Flag, should be investigated for verification. The following Red Flags are potential indicators of fraud. More detailed examples of these indicators are included in the Exhibits at the end of this section.
      1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
      2) The presentation of suspicious documents;
      3) The presentation of suspicious personal identifying information, such as a suspicious address change;
      4) The unusual use of, or other suspicious activity related to, a Covered Account; and
      5) Notice from Customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts held by the financial institution or creditor.
   c. Responding to Red Flags: Known and suspected fraudulent activity must be reported immediately to protect Customers and the University from damages and loss.
      1) Gather all related documentation and complete a Privacy Incident Report, available on the Privacy Office web site; provide a complete description of the situation. Send the report to the UF Privacy Office.
      2) If, after investigation, a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:
         a) Canceling the transaction;
         b) Notifying and cooperating with appropriate law enforcement;
         c) Determining the extent of liability of the University; and
         d) Notifying the Customer that fraud has been attempted.
   d. Violations: Corrective action will be taken in the event of intentional violations of this policy. Such action may include:
      1) Modification of a process, practice, record or record system to better protect the confidentiality of Social Security Numbers, and/or

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Identity Theft Prevention Program (continued)

2) Disciplinary action up to and including termination or expulsion in accordance with University disciplinary policies.

e. Training: University workforce members who have access to consumer reports and/or accounts must be trained concerning Red Flag Rules.
   1) The Privacy Office is responsible for ensuring identity theft training for all requisite workforce members, at hire and annually thereafter.
   2) Employees should receive notice when changes are made to the Identity Theft Prevention Program.

f. Updates to the Identity Theft Prevention Program: At regular intervals, as established in the program or as required, the program will be re-evaluated to include:
   1) An overview of all aspects of the program to be sure they are up to date and applicable in the current business environment.
   2) An assessment of which Accounts are covered by the program.
   3) Revision, replacement or elimination of Red Flags, as well as definition of new Red Flags, as appropriate.
   4) Review of corrective actions, sanctions, and mitigation plans.

g. Oversight Of Service Provider Arrangements
   1) It is the responsibility of University entities that contract for services to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.
   2) A service provider that maintains its own Identity Theft Prevention Program, consistent with the guidance of the Red Flag rules, validated by appropriate due diligence, and included in the service agreement, may be considered to be meeting these requirements.
   3) Any specific requirements should be specifically addressed in the appropriate contract arrangements.

3. Security: The University will implement every reasonable measure to protect restricted data provided to it by individuals, including, but not limited to, creating, maintaining, and using University records and record systems securely so that restricted data are only used and disclosed in accordance with state and federal regulations.

a. Prohibited Activities:
   1) Public display of restricted data. (i.e., to exhibit, hold up, post, or make visible or set out for open view, including but not limited to, open view on a computer device, computer network, website, or other electronic medium or device, to members of the public or in a public manner.)
   2) Using restricted data as the primary account number or identifier for an individual, except where existing University records or record systems require such use. Existing records or records systems, when retired, will be replaced with records or record systems that do not require or use Social Security Numbers or credit card numbers as the primary account number or identifier.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Identity Theft Prevention Program (continued)

3) Visibly printing restricted data on identification cards or badges. (NOTE: This prohibition does not include student UFID's; see the policy for *Privacy of UFIDs* in this manual.)
4) Using, transmitting by any means, including by email, downloading, or storing restricted data in or from records, record systems, or databases that are not encrypted or otherwise secured.
5) Requiring an individual to transmit his/her Social Security Number or credit card information over the Internet or a computer system or network, unless the connection is secure, or the transmission is encrypted.
6) Requiring an individual to use or transmit his/her Social Security Number to gain access to an Internet website or a computer system or network, unless the connection is secure, or the transmission is encrypted.

b. Limited Access: Access to records and record systems containing restricted data is limited to those who have an approved business reason to know this information.
   1) The University limits access to restricted data to employees who have a legitimate University business reason to use or disclose such information or documents. (For more information see: http://www.it.ufl.edu/policies/security/documents/use-limitations-pii.pdf and http://www.it.ufl.edu/policies/security/documents/use-limitations-pci.pdf.)
   2) Unit supervisors/unit administrators are responsible for implementing appropriate unit oversight procedures.

c. Record Disposal: Records containing restricted data must be disposed of in a manner that minimizes the risk of inappropriate access when those documents no longer need to be retained and pursuant to University document retention policies.
   1) Paper documents containing restricted data should be shredded immediately, or placed in secure containers for later secure shredding and recycling.
   2) Electronic documents containing restricted data should be destroyed in a manner consistent with the "best practices" guidance issued by the information technology offices.

❑ **REFERENCES :**

Florida Statutes 119.071(5), 817.568
15 U.S.C. 1681a, 1691a; 18 U.S.C. 1029(e)
16 CFR 603.2(a), 16 CFR 681: Identity Theft Rules ("Red Flag Rules")
§ 334.82(b) Fairness and Accuracy in Credit Transactions Act
Red Flag Program Clarification Act of 2010
UF's Media Reuse and Data Destruction Standard
http://www.it.ufl.edu/policies/security/documents/it-worker-reuse-and-disposal-standards.pdf
UF's Use Limitations of Personally Identifiable Information
http://www.it.ufl.edu/policies/security/documents/use-limitations-pii.pdf

❑ **EXHIBITS :**

Request to Use Social Security Numbers (form)
Red Flag Indicators (chart)

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Identity Theft Prevention Program (continued)

UF UNIVERSITY of FLORIDA

Request to Collect, Use, or Store Social Security Numbers

REQUESTED BY:	
Name of Individual:	Title:
College or Administrative Department	Department, Division or Unit Name and Number:
Telephone #(s):	Email Address:
DESCRIPTION & JUSTIFICATION	
Name & Description of System, Application or Business Process. *Attach copies of all relevant forms, documents, reports, files, etc.*	
Justification for use of the SSN. *Identify any specific legal or regulatory statues that may apply.*	
How will the information be protected in each system, application or business process? *Describe all methodologies that will be used throughout the SSN lifecycle (e.g. collection, storage, retrieval, transmission and disposal).*	
Is the SSN collected directly from the employee, student, customer, etc.? If so, how will the SSN Privacy Notice be provided?	
With whom will the SSN be shared? *Name all entities.* If an external vendor, agency, etc., how will they protect the number? *Describe in detail.*	
When will the use of the SSN be discontinued? *Describe the approach and timeline.*	

Sample Only

Do Not Copy

Access the correct form at:
http://privacy.health.ufl.edu/SocSecNos/index.shtml

APPROVALS: Signatures Required	
Requestor:	Date
Privacy Analyst:	Date
Chief Privacy Officer	Date

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Identity Theft Prevention Program (continued)

Red Flag Indicators	
1. Alerts, notifications or warnings from a consumer reporting agency:	➢ A fraud or active duty alert included with a consumer report; ➢ A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or ➢ A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.
2. Consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or Customer:	➢ A recent and significant increase in the volume of inquiries; ➢ An unusual number of recently established credit relationships; ➢ A material change in the use of credit, especially with respect to recently established credit relationships; or ➢ An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
3. Suspicious Documents:	➢ Documents provided for identification that appear to have been altered or forged. ➢ The photograph or physical description on the identification is not consistent with the appearance of the applicant or Customer presenting the identification. ➢ Other information on the identification is not consistent with information provided by the person opening a new Covered Account or Customer presenting the identification. ➢ Other information on the identification is not consistent with readily accessible information that is on file with the University, such as a signature card or a recent check. ➢ An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
4. Suspicious Personal Identifying Information:	➢ Personal identifying information provided is inconsistent when compared against external information sources used by the University. For example: • **The address does not match any address in the consumer report;** • **The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or** • **Personal identifying information provided by the Customer is not consistent with other personal identifying information provided by the Customer. For example, there is a lack of correlation between the SSN range and date of birth.** ➢ Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example, the address on an application is the same as the address provided on a fraudulent application ➢ Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University. For example: • **The address on an application is fictitious, a mail drop, or a prison; or** • **The phone number is invalid or is associated with a pager or answering service.** ➢ The SSN provided is the same as that submitted by other persons opening an account or other Customers. ➢ The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other Customers or other persons opening accounts. ➢ The Customer or the person opening the Covered Account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete. ➢ Personal identifying information provided is not consistent with personal identifying information that is on file with the University. ➢ When using security questions (mother's maiden name, pet's name, etc.), the person opening the Covered Account or the Customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Red Flag Indicators	
5. Unusual or Suspicious Activity	➢ Shortly following the notice of a change of address for a Covered Account, the University receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account. ➢ A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the Customer fails to make the first payment or makes an initial payment but no subsequent payments ➢ A Covered Account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: • **Nonpayment when there is no history of late or missed payments;** • **A material change in purchasing or usage patterns** ➢ A Covered Account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors). ➢ Mail sent to the Customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Customer's Covered Account. ➢ The University is notified that the Customer is not receiving paper account statements. ➢ The University is notified of unauthorized charges or transactions in connection with a Customer's Covered Account. ➢ The University receives notice from Customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts held by the University ➢ The University is notified by a Customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations

❑ **POLICY** Rev: 02/01/2012

1. ***Privacy Incidents and Complaints:*** The University of Florida will review or investigate and attempt to resolve all complaints and confirmed incidents relating to breaches of privacy and confidentiality within a reasonable time after a complaint is received or a privacy incident is reported. Incidents and complaints must be filed within 180 days of the time the violation was known, or reasonably should have been known, to have occurred.

2. ***Non-Retaliation:*** The University of Florida will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or reporting a privacy incident, or inquiring about how to file a complaint or incident report.

3. ***Designated Personnel:*** The University of Florida will designate staff to review and determine action on privacy complaints and incident reports filed with the University. These designated staff will also perform these functions when the University of Florida is contacted about complaints filed with the Office of Civil Rights (HIPAA) or the Family Policy Compliance Office (FERPA).

4. ***Documentation:*** The University of Florida will document all privacy complaints and reported privacy incidents.
   a. Documentation will include:
      1) The findings from reviewing each complaint and incident,
      2) A description of corrective actions taken, or an explanation of why corrective actions are not needed,
      3) A description of risk assessments completed when restricted or sensitive data is involved,
      4) Any notification procedures taken, including recommendations and final approvals, and
      5) Any mitigation undertaken for each specific reported complaint or incident.
   b. Documentation for all privacy complaints and reported incidents will be maintained for at least six years, or longer if required by law or other circumstances.

5. ***Notification:*** The University will make reasonable efforts to notify affected persons if it is determined that their personal identification information was, or is reasonably believed to have been, acquired by an unauthorized person and that the information could be used for fraudulent purposes.
   a. The Chief Privacy Officer determines, either alone or with the assistance of the Notification Recommendation Team, whether individuals affected by a privacy breach must be notified as required by Florida Statutes. Affected individuals will be notified without unreasonable delay, but no later than 45 days after the determination is made.
   b. Notification to affected individuals will include the following components. The notification will also be posted on the UF Privacy website, if appropriate.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

1) A general description of the incident;
2) The Police Report number, if available,
3) Instructions and necessary information for notifying the major credit agencies of suspected or potential identity theft.
4) The University's Privacy Office telephone numbers, including the Hotline, and website information.

c. While the UF Privacy Office will oversee the notification process, the College, Department, Division, Clinic, or other University unit from which the information was acquired will be responsible for the costs and labor associated with notifying the affected persons.

6. ***Investigations and Disciplinary Action:*** The Chief Privacy Officer or designee is responsible for investigating all suspected violations involving restricted information created and maintained by the University of Florida and its affiliated entities.

a. Every effort will be made to complete Investigations within 30 business days.

b. The Chief Privacy Officer recommends sanctions for confirmed violations to Department Chairs, considering the following factors:
   1) The facts of the investigation:
   2) The nature of the violation,
   3) The severity of the violation,
   4) Whether the violation was intentional or unintentional, and
   5) Whether the violation indicates a pattern or practice of improper use or disclosure of private data.
   6) The precedents of earlier sanctions;
   7) The approved sanction guidelines

c. Sanctions may range from a verbal warning to separation from employment or expulsion from the University, in accordance with applicable Florida Labor Laws, Florida Administrative Code, and/or University of Florida Rules as appropriate.

d. All privacy-related sanctions that are applied by the University of Florida will be documented in the employee's personnel file or the student's education record, as appropriate.

e. The Chief Privacy Officer will consult with University of Florida expertise, if necessary, to assist with recommendations for sanctions, corrective actions, and mitigation. Members of the panel may include, but are not limited to, representatives from Human Resources, Risk Management, Health Science Center Administration, the Office of General Counsel and other UF administrative representatives as appropriate.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

❑ PRIVACY DEFINITIONS

Breach: An actual violation of applicable law and/or UF policy or procedure; going against established rules, including, without limitation, an "unlawful and unauthorized acquisition of… data that materially compromises the security, confidentiality, or integrity of personal information maintained by [an entity]. Good faith acquisition of personal information by an employee or agent of the [entity] is not a breach or breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use." (F.S. 817.568(4))

Mitigation: To make less severe, to partially remove, or to correct, so that harmful effects of a privacy violation are reduced or eliminated.

Notification: The act of informing persons affected by a breach of private information that their information was included and steps they can take to protect themselves and their privacy.

*Personal Identification Information: "*Any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including, [but not limited to]: any name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name,… driver's license or identification number,… passport number,… credit or debit card number,… unique biometric data, such as fingerprint, voice print, retina… image,… medical records, telecommunication identifying information or access device; or other number or information that can be used to access a person's financial resources." (F.S. 817.568(1)(f)) ***Please note that Personal Identification Information and Personal Information are defined differently for notification purposes****.*

Personal Information: As defined by Florida Statute 817.5681(5) and for which notification is required, if breached: "An individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:

1. Social security number.
2. Driver's license number or Florida Identification Card number.
3. Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"For purposes of this section, the term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media."

Privacy Complaint: An allegation by an individual that an organization is not complying with the requirements of the federal privacy and/or security regulations or the organization's own policies and procedures related to the privacy / security of personal information.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

Privacy Incident: A known or suspected action, inconsistent with the organization's privacy policies and procedures, or an adverse event, related to restricted or sensitive information.

- **IT PRIVACY DEFINITIONS**

Access (to Information): The ability or the means necessary to read, write, modify, or communicate data or information or otherwise make use of any system resource.

Authorized Access: Rights granted to an individual to allow access to information.

Authorized Disclosure: The permissible release, transfer, provision of, access to, or, divulging in any other manner of information by any means of communication outside the entity holding the information.

Compromise: Access in excess of that intended to be available.

Data Processing Software: The programs and routines used to employ and capabilities of data processing hardware, including but not limited to, operating systems, compilers, assemblers, utilities, library routines, maintenance routines, applications of networking programs.

Information system: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Information Technology Resources (Florida Chapter 119.011): IT Resources means data processing hardware and software communications, supplies personnel, facility resources, maintenance, and training.

IT Resource: Any equipment that has the primary purpose to store, process, display or transport digital information. The associated data, applications and hardware, are also IT resources.

Need-to-Know: Approved access to, or knowledge or possession of specific information required to carry out official duties by officers and employees of the enterprise that maintains the data.

Reasonable Person Standard (agreed to 5-8-06): Phrase to denote a hypothetical person who exercises qualities of attention, knowledge, intelligence and judgment that society requires of its members for the protection of their own interest and the interest of others. (i.e. A test for negligence is based on either a failure to do something that a reasonable person, guided by considerations that ordinarily regulate conduct, would do, or on the doing of something that a reasonable person would not do.)

Risk of Potential Harm: Undesired consequences of an action or event, capable of developing into an actuality, that causes physical or psychological/emotional damage to an individual. Harm is any detriment caused by a violation of a legal interest, as a result of a certain technical process or state.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operation, in an information system.

Valid Business Purpose: Assigned job activities require the active use of authorized access to view, read, modify, possess, or communicate data or information, or involve common but passive encounters with the data or information.

❑ **PRIVACY REQUIREMENTS**

1. A person who believes the University of Florida is not complying with the requirements of federal or state privacy regulations may file a complaint with the University's Chief Privacy Officer. (If protected health information (PHI) is involved, a Health Information privacy complaint may also be filed with the U.S. Secretary of Health and Human Services. (See: Health Information Privacy Operational Guidelines: Complaints))
2. The University must provide a process for individuals to make complaints or to report incidents regarding the University's information privacy and security procedures. The University must document all complaints and privacy incident reports received and their disposition.
3. The University must notify any resident of the State of Florida of any breach of the security of a computerized data system that includes unencrypted personal information, if it is determined that the information was, or is reasonably believed to have been, accessed by an unauthorized person. (F.S. 817.5681(1)(a))
4. The University will apply appropriate sanctions against members of its workforce who fail to comply with the University's privacy and security policies and procedures or with federal and state privacy and security regulations.
5. The University will mitigate, to the extent practicable, any harmful effect of a confirmed health information privacy violation.

❑ **PROCEDURES:**

1. Investigating Privacy Complaints and Incidents:

a. Privacy Complaints: The Chief Privacy Officer or designated representative will:
   1) Initiate a formal investigation upon receipt of a formal verbal complaint or a completed Privacy Complaint form. The complainant should complete a written Complaint form for this purpose.
   2) Contact the complainant, preferably by telephone, within three (3) business days of receiving written notice of a complaint if prior contact has not already been made.
   3) Document any conversations with the complainant, any alleged perpetrators and witnesses, including the date, time, and a general summary of each dialogue.
   4) Attach relevant materials or statements to the investigation documents.
   5) File the completed Complaint investigation and resolution documentation in the Privacy Office and maintain for at least six years.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

Note: If the complainant is a patient, student, employee, or otherwise associated with the University, the documentation is not included in the complainant's personal medical, personnel, or academic records.

b. Privacy Incidents: The Chief Privacy Officer or designated representative will:
   1) Upon receipt of a report of a Privacy Incident, review the matter, and then initiate a formal investigation, if warranted. The person notifying the Privacy Office should complete a Privacy Incident Report form for this purpose.
   2) Document any conversations with the person who reported the incident and any alleged perpetrators or other responsible parties, including the date, time, and a general summary of each dialogue.
   3) Determine whether the subject (person whose private information is affected) is aware of the alleged incident:
      a) If fewer than ten (10) subjects are involved, and the subjects are aware of the alleged incident, make every effort to contact the subject(s) within five (5) business days of receiving the incident report if prior contact has not already been made. The method of contact is at the discretion of the Chief Privacy Officer. Document the contact, and include the date, time and a general summary of any conversations or messages left or received.
      b) If the subject is not aware of the alleged privacy incident, investigate the incident thoroughly before determining whether the subject should be informed.
      c) If more than ten (10) subjects are involved, refer to the notification procedures following.
   4) File the completed Privacy Incident investigation and resolution documentation in the Privacy Office and maintain for at least six years.

   Note: If the subject is a patient, student, employee, or otherwise associated with the University, the documentation is not included in their personal medical, personnel, or academic records.

2. Actions To Be Taken By the Chief Privacy Officer When No Privacy Violation Is Found

a. Documentation: If after investigation of either a complaint or an incident, it is determined that no federal or state privacy or security regulations, and no privacy/security policies of the University of Florida, have been violated, document the findings and recommended actions (if any) in appropriate reports.

b. Notification:
   1) For Privacy Incidents where no violation is found, notify the person whose information was involved only if they were already aware of the potential violation and that it was being investigated. Document any conversations, and provide written records of the incident resolution, as appropriate.
   2) For Privacy Complaints where no violation is found, notify the complainant upon conclusion of the investigation and explain the findings; provide a written record of the complaint resolution.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

a) Document the response to the notification, specifically, whether the person was satisfied or dissatisfied with the disposition of the complaint/incident.
b) If the person is not satisfied, refer the matter to the University of Florida's legal counsel as well as any other University personnel directly involved, as necessary and appropriate.

3. Actions To Be Taken By the Chief Privacy Officer When A Privacy Violation Is Found

a. Documentation: If after investigation it is determined that state or federal regulations and/or privacy/security policies of the University of Florida have been violated document the findings and recommended actions in appropriate reports.

b. Corrective Action: Recommend a corrective action and recovery plan, including any plans for mitigation, where appropriate. Convene and direct a panel of University of Florida expertise for this purpose, when necessary.

c. Notification: Privacy Complaints:
   1) Upon conclusion of the investigation, meet with or contact the complainant and explain the findings; provide a written record of the complaint resolution.
   2) Document the complainant's response (whether the complainant is satisfied or dissatisfied with the disposition of the complaint).
   3) If the complainant is not satisfied with the disposition of the complaint, refer the matter to UF's legal counsel and any other University personnel directly involved (if necessary and appropriate).

d. Notification: Privacy Incidents
   1) Determine if notification is required:
      a) Using the Risk Assessment procedure (following), the Chief Privacy Officer determines whether notification is necessary and proceeds as determined.
         i. Where the probability of exposure is "Certain" (confirmed data taken and/or unauthorized exposure), the Chief Privacy Officer, along with members of IT Security, makes the notification determination.
         ii. Where the probability of exposure falls into categories of "Remote", "Possible", or "Likely", the Chief Privacy Officer must convene the Core Notification Recommendation Group.
      b) When the Chief Privacy Officer convenes the Core Notification Recommendation Group, they use the Notification Risk Assessment Procedure and the Notification Matrix to determine together whether notification of the affected individuals is necessary. (See the Notification Risk Assessment Procedure, following.)
   2) If the person(s) whose information was involved is not to be notified of the confirmed privacy incident, the Chief Privacy Officer documents the details of this decision.
   3) Notify affected individuals of the confirmed privacy violation in writing as follows:

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

a) Notify the appropriate UF Administration, as well as Public Relations, News & Communications, Risk Management, and the Vice President for Human Resources, immediately.
b) Assist the College, Department, Division, Clinic, or other University unit to notify all affected persons (patients, students, employees, legal representatives, etc.) as soon as is practicable.
   i. Notification must conform to the requirements of F.S. 817.5681.
   ii. While the Privacy Office will oversee the notification process, the College, Department, Division, Clinic, or other University unit from which the information was acquired will be responsible for costs and labor associated with notifying the affected persons.
c) Document all subsequent conversations with the affected individuals, and provide them with written records of the incident resolution, as appropriate.

4. ***Notification Risk Assessment Procedure:*** Use the following process to make a 'notification' decision following an actual or suspected disclosure of Restricted data.
   a. <u>Notification Recommendation Team:</u>
      1) Core Members:
         a) UF Chief Information Officer or UF Chief Security Officer
         b) UF Chief Privacy Officer
      2) Ex-officio: Office of General Counsel
      3) Ad hoc:
         a) University Police Department
         b) University News and Public Relations
         c) UF Information Security Forensic Team
         d) UF Data Principal of the information related to the investigation
   b. <u>Impact Considerations:</u> Consider the impact to UF assets such as its financial assets (costs), its reputation, and in extreme cases the freedom of a workforce member in the event of an incident with criminal implications.
      1) Cost and Liability Considerations:
         a) Legal and liability expenses (reserves)
         b) Restitution for loss (victim financial damages)
         c) Operational expenses to handle fallout, to resume business operation, etc.
         d) Sanctions, fines, penalties assessed
         e) Opportunity losses (donations, grants)
         f) Potential for indictment and incarceration
      2) Reputation Considerations:
         a) Damage to victims (sensitive nature of the data)
         b) Whether the reputation damage to UF will be minimal, short term or long term
      3) Media and Public Interest Considerations:
         a) Local – community, county, Gainesville and Jacksonville
         b) Regional – State wide or south eastern US
         c) National news interests

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

c. Probability Considerations: Consider evidence of the intruder's capabilities for accessing the data, evidence of opportunity to access and/or use the data, and evidence of the intruder's intention to access and/or use the data.
   1) Capability of intruder or unauthorized accessor:
      a) Privileges the intruder was able to assume
      b) Electronic "footprints" of intruder – activity, files installed
      c) Adequacy of controls that were in place at the time of the breach
   2) Opportunity for intruder or unauthorized accessor to access:
      a) Privileges the intruder was able to assume
      b) Duration of intruder's presence on the system
      c) Duration of intruder's activities
      d) Access date/time stamps of Restricted and Sensitive data
   3) Intent or motivation of intruder or unauthorized accessor:
      a) Misuse of computer resources
      b) Data theft
      c) Hardware theft
      d) Thrill
   4) Misplaced data considerations (i.e. data on removable media or portable computer):
      a) Accidentally discarded (type of media will be a factor; discarded hard drive or memory stick is more likely to result in an unauthorized disclosure than a discarded CD, DVD or floppy disk.)
      b) Location is forgotten (again media will be a factor; misplaced laptop or PDA is more likely to result in an unauthorized disclosure than misplaced removable media.)
      c) Recovery likelihood

d. Risk Descriptions and Recommended Actions
   1) High: The risk analysis indicates high risk to the institution if it does not notify the victims. The Chief Privacy Officer and/or Core Team must recommend notification.
   2) Moderate: The risk analysis indicates risk to the institution if it does not notify the victims.
      a) Consider notifying if the institution believes the breach may reach the public and it wishes to pre-empt with facts for damage control.
      b) Notification recommendation is determined by a consensus of the Core Team with dissenting opinion going forward with the recommendation.
   3) Low: The risk analysis indicates a low risk to the institution if it does not notify the victims. The Chief Privacy Officer and/or Core Team may still recommend notification.

e. Recommendations and Final Approval: Upon completion of the recommendation the Core Team forwards it to the Senior Vice-President for Administration for approval, unless functional responsibility is specifically delegated (i.e., Chief Privacy Officer).

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

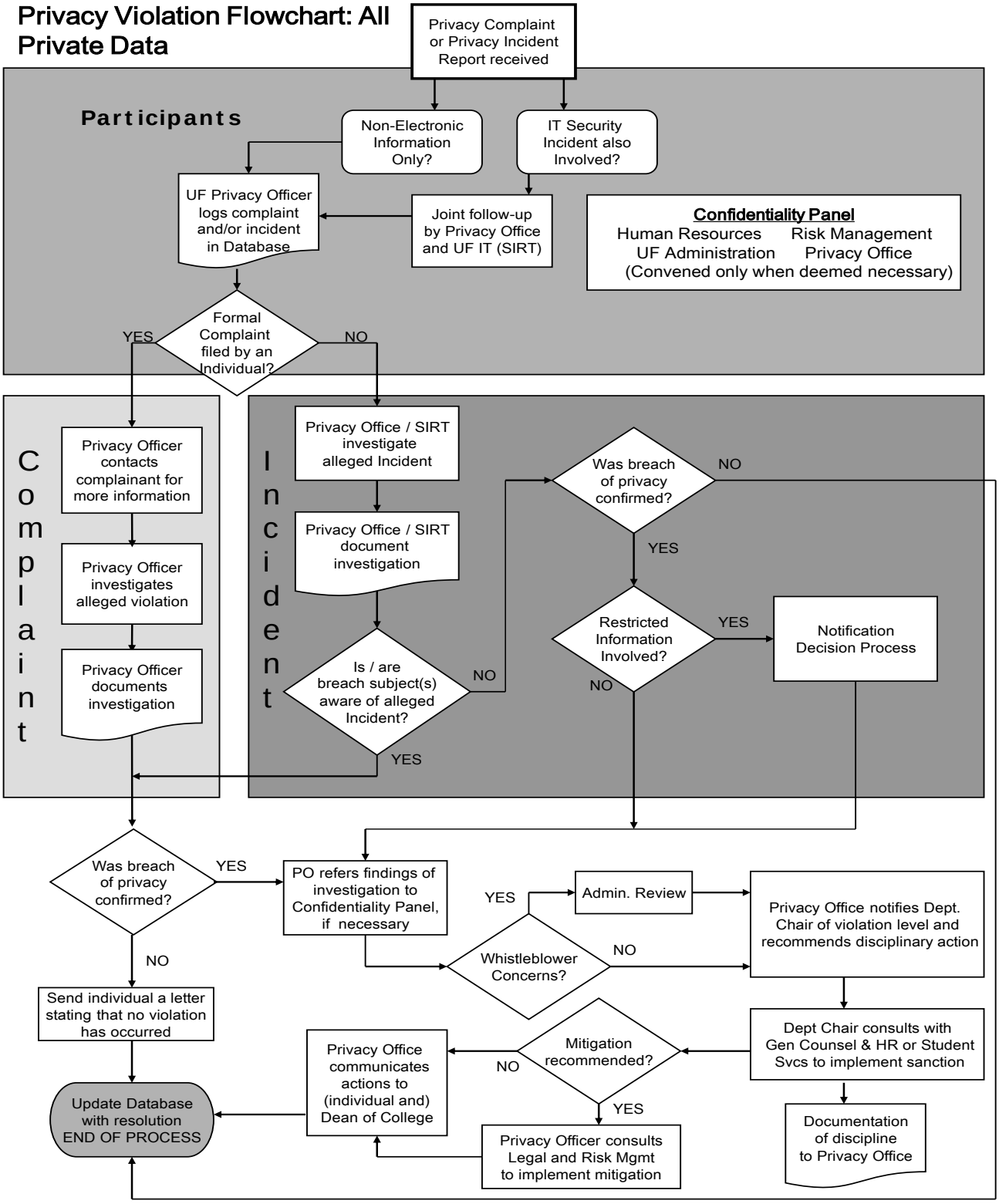
- **REFERENCES:**

  HIPAA Regulations: 45 CFR § 160.306 (Complaints to the Secretary) and § 164.530(d) (Complaints), (e) (Sanctions), and (f) (Mitigation)
  Florida Statutes: 817.568 & 817.5681 (Criminal use of personal information)
  University Regulations: Rules 6C1-1.008(1)(o), 6C1-3.047(3)(d), 6C1-4.016(2)(o) and (t), and 6C1-7.048(1)(c)

- **EXHIBITS:** Privacy Violation Flowchart
  Notification Flowchart
  Sanctions Matrix: Faculty and Staff
  Sanctions Matrix: Students
  Information from Federal Trade Commission website
  Privacy Incident / Complaint Summary Report

© Copyright 2003 - 2008. University of Florida. All rights reserved.

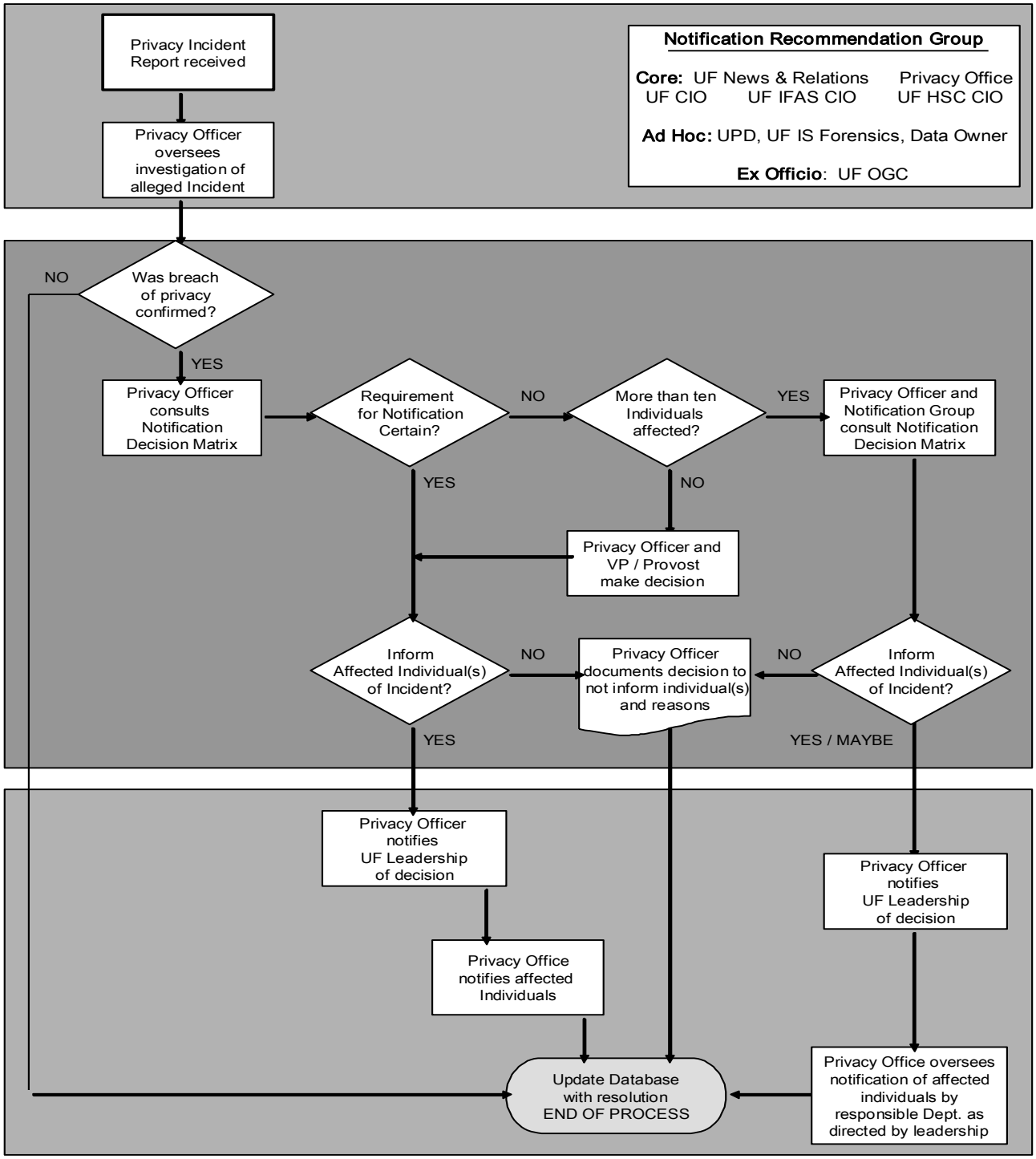
Investigating and Responding to Privacy Violations (continued)



© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

Notification Process Flowchart
Restricted Electronic Information



© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

Recommended Sanctions for Violations of Privacy by Faculty and Staff

Rev: 8/15/2007

Level of Violation	Cause or Motivation	Type of Violation	Examples of Violations	Recommended Actions
Level I Errors in handling Restricted or Sensitive information, or in maintaining workstation security measures.	Unintentional • Lack of training • Inexperience • Poor judgment • Poor process	• Clerical Error • Process Error • Technical Error • Judgment Error	• Leaving an active computer screen with access to PII unattended. • Leaving PII, in any format, unattended in public areas. • Disclosing PII without identity verification. • Sending PII to wrong postal or e-mail address • Placing non-shredded documents in inappropriate waste receptacles	• Retraining and re-evaluation. • Specialized training and evaluation. • Discussion of policy and procedures. • Verbal warning or oral reprimand. • New Confidentiality Statement signed
Level II Breach in the terms of the Confidentiality Statement and/or UF policies concerning use and disclosure of Restricted or Sensitive Information.	Intentional, but non-malicious • Curiosity • Concern • Compassion • Carelessness • Compulsiveness	• Un-authorized • Non-job-related • Stealth	• Failure to complete required Privacy Training and/or to sign the UF Confidentiality Statement. • Discussing PII in public or other inappropriate areas. • Accessing the record of any person, including co-workers, friends, or family, without professional Need-to-Know • Using someone else's computer account. • Copying information as a favor • Installing unauthorized software with potential to harm systems. • Adding, deleting, or altering electronic information without authorization. • Repeated Level I violations	• Letter of Reprimand requiring written corrective action plan in response; ineligible for bonus, transfer or promotion for 6 to12 months. • Suspension of information system user privileges • Suspension of employment
Level III Breach in the terms of the Confidentiality Statement and/or UF policies concerning use and disclosure of Restricted or Sensitive Information, for personal gain or to affect harm on another person.	Malicious intent • Financial gain • Revenge • Protest Gross Negligence	• Theft, including Identity theft • Malicious actions: i.e., ○ alteration or deletion of data, ○ making data or systems inaccessible	• Access and unauthorized disclosure of PII for personal gain or to affect harm on another person. • Unauthorized access of celebrity or VIP PII for any reason. • Malicious alteration, deletion or removal of PII, from UF facilities. • Unauthorized publication or broadcasting of PII. • Repeated Level I or II violations	• Final written warning and/or • Termination of information system user privileges • Revocation of Medical Staff privileges. • Termination of employment: ineligible for rehire and future information systems access.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

Recommended Sanctions for Violations of Privacy by Students

Rev: 8/15/2007

Level of Violation	Cause or Motivation	Type of Violation	Examples of Violations	Recommended Actions
Level I Errors in handling Restricted or Sensitive information, or in maintaining workstation security measures.	Unintentional • Lack of training • Inexperience • Poor judgment • Poor process	• Clerical Error • Process Error • Technical Error • Judgment Error	• Leaving an active computer screen with access to PII unattended. • Leaving PII, in any format, unattended in public areas. • Disclosing PII without identity verification. • Sending PII to wrong postal or e-mail address • Placing non-shredded documents in inappropriate waste receptacles	• Retraining and re-evaluation. • Specialized training and evaluation. • Discussion of policy and procedures. • Verbal warning or oral reprimand. • New Confidentiality Statement signed • Community Service, as appropriate
Level II Breach in the terms of the Confidentiality Statement and/or UF policies concerning use and disclosure of Restricted or Sensitive Information.	Intentional, but non-malicious • Curiosity • Concern • Compassion • Carelessness • Compulsiveness	• Un-authorized • Non-job-related • Stealth	• Failure to complete required Privacy Training, and/or to sign the UF Confidentiality Statement. • Discussing PII in public or other inappropriate areas. • Accessing the record of any person, including co-workers, friends, or family, without professional Need-to-Know • Using someone else's computer account. • Copying information as a favor • Installing unauthorized software with potential to harm systems. • Adding, deleting, or altering electronic information without authorization. • Repeated Level I violations	• Letter of Reprimand, requiring written corrective action plan & acknowledgement of consequences of subsequent infractions; i.e., expulsion, and obligation to make restitution, as appropriate. • Loss of University privileges, including use of University library, parking, computers, and athletic / entertainment functions. • Conduct Suspension • Contract of Restitution
Level III Breach in the terms of the Confidentiality Statement and/or UF Policies concerning use and disclosure of Restricted or Sensitive Information, for personal gain or to affect harm on another person.	Malicious intent • Financial gain • Revenge • Protest Gross Negligence	• Theft, including Identity theft • Malicious actions: i.e., ○ alteration or deletion of data, ○ making data or systems inaccessible	• Access and unauthorized disclosure of PII for personal gain or to affect harm on another person. • Unauthorized access of celebrity or VIP PII for any reason. • Malicious alteration, deletion or removal of PII, from UF facilities. • Unauthorized publication or broadcasting of PII. • Repeated Level I or II violations	• Expulsion without opportunity to continue at the University in any status, and ineligible for University privileges, including use of University library, parking, and entertainment / athletic functions. • No Contact Order • Contract of Restitution

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

Information from the Federal Trade Commission's Website:

If you think your identity has been stolen, here's what to do:

1. Contact the fraud departments of any one of the three consumer reporting companies to place a "fraud alert" on your credit report. The fraud alert tells creditors to contact you before opening any new accounts or making any changes to your existing accounts.

You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports.

2. Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit form, found on the Federal Trade Commission's website, when disputing new unauthorized accounts.

3. File a report with your local police or the police in the community where the identity theft took place. Get a copy of the report or at the very least, the number of the report, to submit to your creditors and others that may require proof of the crime.

4. File your complaint with the FTC. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps us learn more about identity theft and the problems victims are having so that we can better assist you.

What is a fraud alert?

There are two types of fraud alerts: an **initial** alert, and an **extended** alert.

• **An initial alert stays on your credit report for at least 90 days.** You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide consumer-reporting companies.

• **An extended alert stays on your credit report for seven years.** You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an "identity theft report." When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer-reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list before then.

To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your Social Security number, name, address and other personal information requested by the consumer reporting company.

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

Information from the Federal Trade Commission's Website (continued)

When a business sees the alert on your credit report, they must verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. This may cause some delays if you're trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

Consider Requesting a Credit Freeze

You may want to contact the credit reporting companies to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely an identity thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. In many states, identity theft victims can place a freeze for free, but in others, victims must pay a fee, which is usually about $10. If you have a police report, you may be able to place or lift a freeze for free. Putting a credit freeze on your credit file does not affect your credit score. If you place a credit freeze on your credit file, you can:

- get a copy of your free annual credit report
- open a new account, apply for a job, rent an apartment, buy insurance, refinance your mortgage, or do anything else that requires your credit report

If you want a business, lender, or employer to be able to review your credit report, you must ask the credit reporting company to lift the freeze. You can ask to lift the freeze temporarily or permanently. You may be charged a fee to lift the freeze.

Important Contact Information

There are a number of helpful services to help you respond if you have been a victim of identity theft. Below is a list of resources that we have compiled on your behalf.

Federal Trade Commission's Identity Theft Hotline
The FTC operates a call center for ID theft victims where counselors tell consumers how to protect themselves from identity theft and what to do if their identity has been stolen. (1-877-IDTHEFT [1-877-438-4338]; TDD: 1-866-653-4261; or http://www.consumer.gov/idtheft)

FTC ID Theft Brochure: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf

Equifax: 1-800-525-6285; www.equifax.com;
P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com;
P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com;
Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

© Copyright 2003 - 2008. University of Florida. All rights reserved.

Investigating and Responding to Privacy Violations (continued)

SUMMARY REPORT
PRIVACY INCIDENT / COMPLAINT / PATIENT REQUEST To be completed by the Chief Privacy Officer or Designee

For Complaint / Incident / Patient Request reported on (date): _____ **Concerning:**		
RESPONSE to COMPLAINT/ INCIDENT:		
Privacy Violation Identified: ___ YES ___ NO	**Level:** I II III NA	
Type of Violation:		
STATEMENTS / INPUT FROM WITNESSES ATTACHED:		
NAME:	**NAME:**	
NAME:	**NAME:**	
NAME:	**NAME:**	
SANCTIONS COMMITTEE CONVENED ON:	___ Notes Attached	
RECOMMENDATION FOR CORRECTIVE ACTION:		
RECOMMENDATION FOR DISCIPLINARY ACTION:		
RECOMMENDATION FOR MITIGATION:		
OTHER NOTES:		
OTHER ATTACHMENTS:		
INVESTIGATION COMPLETED:	**REPORTING COMPLETED:**	**CLOSED:**
Completed by: _____	**Date:** _____	

© Copyright 2003 - 2008. University of Florida. All rights reserved.