University of Central Florida

Information Security Office

ISO SOP 605 – Incident Response for Breach of Restricted Personal Data

Date Created: August 3, 2010

Last Updated: June 23, 2011

CONTENTS

OBJECTIVE

Procedures and guidelines for responding to data security breaches, and internal and external reporting requirements.

SCOPE

Procedure applies to data security breaches for restricted personal data as defined by UCF policy 4-008.

PROCEDURES

INTERNAL REPORTING

What is a Reportable Incident?

A reportable incident occurs when

1. an unauthorized person is believed to have gained the ability to access restricted personal or confidential data that is stored on a university system
2. a person who is authorized to access restricted personal or confidential data that is stored on a University system misuses that data.
3. Until proven legitimate, false-positives must be recorded and documented as an incident.

Restricted Personal and Non-Personal Data

Restricted personal and non-personal data are defined in the University's Data Classification and Protection Policy, policy 4-008. Restricted personal and non-personal data include:

1. Social security number
2. Credit card number or debit card number
3. Bank account number, automated clearing house number, or electronic funds transfer account number
4. Driver's license number
5. Name, address, and date of birth
6. Mother's maiden name
7. Student records that are protected by the Family Educational Rights and Privacy Act (FERPA)
8. Protected health information under the Health Insurance Portability and Accountability Act (HIPAA)
9. Research data or results prior to publication or the filing of a patent application
10. Information subject to a contractual confidentiality provision
11. Security codes, combinations, and passwords

How to Report: College/Department/Business Unit Responsibilities

The College, Department or the Business Unit responsible for the affected data will immediately inform the Information Security Office, and the Security Incident Response Team, of the reportable incident. This contact should be made through the Service Desk of Computer Services & Telecommunications at 407-823-5117, servicedesk@ucf.edu, and sirt@ucf.edu.
SIRT will record the incident in the incident tracking system and if necessary may take a snapshot of the network. If the incident involves a system and an active attack, the system will be removed from the network

The College, Department or the Business Unit responsible for the affected data will conduct the investigation of the reportable incident under the guidance of the Security Incident Response Team (SIRT) and the security incident response procedures and provide a detailed report of the incident, which would include date and time of the incident, type of information disclosed, how it was disclosed, and number of users potentially affected.

Information security breach report form needs to be used to provide the report:
https://publishing.ucf.edu/sites/itr/cst/Documents/infosec/Information_Security_Breach_Reporting_Form.doc

Reporting Responsibilities

Information Security Office will immediately report the incident to the Vice Provost for Information Technology & Resources. The Vice Provost will notify appropriate executives of the university, namely the Provost, the General Counsel's Office, University Audit and other members of the University.

Information Security Office will also promptly report the incident to the following offices depending on the type of information is involved:

- Student records – Registrar’s Office and Institutional Research
- Credit or debit card data – Controller’s Office
- Research, intellectual property, or export-controlled data – Vice President for Research and Commercialization
- Protected health information – HIPAA Privacy Officer
- Employee records – Human Resources Director

These offices are responsible for notifying external parties, e.g., payment card companies and governmental agencies, Department of Education, etc.

EXTERNAL NOTIFICATION OF A SECURITY BREACH

State of Florida (2009 Florida Statutes: **817.5681**) prescribes to all businesses conducted in the state and maintains computerized data in a system must give notice of a data system security breach to individuals whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person in connection with that data system security breach. The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section.

Furthermore, notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.

The following guidelines serve as the University’s notification policy.

Deciding Whether to Notify Affected Persons

When a data security breach involves the acquisition of personal information by an unauthorized person is detected, the University executives (President, Vice Presidents, OGC, etc.) will need to decide whether to notify potentially affected persons.

Personal Restricted Information

Personal information means a person’s first name or first initial and last name in combination with any of the following data elements when the data elements are not encrypted:

- Social security number
- Driver’s license number
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to a person’s financial account
- PID (Personal ID) and password
- NID (Network ID) and password

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Reasonable Belief of Acquisition

In determining whether unencrypted personal information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person, University administrators should consider the following questions:

1. Is the medium or device storing personal information in the physical possession or control of an unauthorized person (e.g., a lost or stolen computer)?
2. Is there credible evidence that personal information has been downloaded or copied?
3. Was personal information used by an unauthorized person (e.g., opening fraudulent accounts or identity theft)?
4. Was the intrusion stopped while in progress, or before personal information could be acquired?
5. Is there credible evidence that the purpose of the intrusion was to seek and collect personal information?
6. Is there credible evidence that the medium or targeted device was used, or being prepared for use, for malicious purposes other than acquisition of personal information (e.g., storage and distribution of large data files)?
7. What is the likelihood that notification would unduly increase the risk of misuse of personal information?
8. What is the likelihood that the intruder has obtained data in a usable format?

Depending on the circumstances, other criteria also may be considered (e.g., potential damage to persons whose personal information may be at risk, ease of notification.)

It is also important to note how the FL state statutes defines the term security "breach" and "breach of the security of the system": It is the unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person (UCF.) Good faith acquisition of personal information by an employee or agent of the person 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.

Notification

In the event that University executives determine that notice of a data security breach to potentially affected persons is warranted, the following procedures will be used.

1. Notice will be provided either by US mail or by e-mail, if a valid e-mail exists and the subject person has agreed to accept communications electronically, without unreasonable delay after detection of the breach. State statutes dictate that notification must be within 45 days.
2. If the cost of giving written notice is excessive, or if there is insufficient contact information to notify a potentially affected person in writing, the University may consider giving notice by one or more of the following methods:
    a. Conspicuous posting of the notice on a University website
    b. Notice in the form of a press release to media

3. The College, Department or the Business Unit responsible for the data affected by the security breach will prepare the communication notice (e.g., letter of apology, explanation, etc. - samples are available from the ISO) which will be reviewed by University administration, e.g., Provost, VP of IT&R, News & Information, OGC, Dean/Director, etc.
4. The liability for the costs associated with production and dissemination of the notification letter are the responsibility of the College, Department or the Business Unit responsible for controlling access to and security of the data.
5. If a press release is issued, the College, Department or the Business Unit responsible for the data affected by the security breach will field the calls and provide information from a FAQ sheet. If a large number of calls are anticipated, the University may contract with an external agency to respond to calls.
6. The College, Department or the Business Unit responsible for the security of the data will bear all costs associated with notification.

DEFINITIONS

CIO. Chief Information Officer, Vice Provost for Information Technologies and Resources (IT&R)
CTO. Chief Technology Officer, Director of Computer Services & Telecommunications, division of IT&R
DSC. Departmental Security Coordinator, security liaison to central IT and ISO.
DOE. Department of Education
FERPA. Family Educational Rights and Privacy Act
ISO. Information Security Office, division of Computer Services & Telecommunications and Information Technologies and Resources.
Restricted Data. Data protected by law, contract or policy, as defined in the Data Classification and Protection Policy, Policy 4-008
Security Incident. incident or finding that can potentially leave restricted data unprotected or lead to unauthorized disclosure.
SIRT. Security Incident Response Team