Incident Response and Investigation (ISSP-002)

Introduction

This document outlines the procedures taken during incidents involving data security at the University of South Florida

Reporting an Incident

Reporting compromises and breaches of security must be made by notifying one of the members of the Incident Response Team (IRT). This notification can be done by sending an email to abuse@usf.edu or by phone at (813) 974-2287. Updated contact information is listed on the USF Security Website at https://security.usf.edu.

Once the report is received, a trouble ticket will be generated and a first summary of the incident will be forwarded to the Information Security Officer (ISO) and to the Information Security Administrator (ISA) responsible for the computer involved in the breach. Members of the Incident Response Team are available to help ISO’s and ISA’s to resolve the issues in a quick and thorough manner. The ISO or the ISA will notify the members of the IRT when the issue has been resolved, and the trouble ticket will be closed.

Incident Involving Restricted Data

Incidents involving resources considered “restricted,” as defined on standards document ISSP-001, must be treated a bit differently. All incidents involving restricted data must be communicated immediately to members of the IRT.

Containment

Members of the IRT will work with local ISO’s and ISA’s to contain the break in as soon as possible. The leak of restricted information must be stopped and further hacker incursions into the compromised resource prevented. Resources considered “deferrable,” as defined on standards document ISSP-001, must be pulled off the network immediately. “Essential” and “required” resources will be allowed to remain connected as long as members of the IRT are confident that the information seepage can be contained. If that is not possible, these resources must also be removed from the network.

Notifications

At the same time the containment is put in place, the following groups will receive a message containing a summary description of the incident. Follow up messages will be sent as the situation develops. The recipients of this message will be instructed not to share this information with any other parties until more details on the extent of the breach are confirmed.

- Members of the Information Security Workgroup (ISW) as needed
- Vice President, Information Technology
- Local ISO’s and ISA’s

The Provost and the University Registrar will also be notified if the data involved in the incident is covered by the Family Educational Rights Privacy Act (FERPA). The local ISO responsible for the resource will be responsible for notifying other members of his or her organization who must be aware of the occurrence.
**Investigation**

Once the local administrators have regained control of the machine, a complete investigation will begin. A copy of the computer's hard drive will be made and kept in a safe in case it is needed for criminal or civil lawsuits. A detailed forensic analysis will be made. Results of the analysis will be correlated with network data and information obtained during personal interviews and emails with the computer's administrators. The goal of the investigation is two-fold:

1) Determine the method used by the hackers to gain access to the machine

2) Discover the total extent of the breach

During the course of the investigation recommendations will be made to the ISO and ISA on how to improve the security of the compromised system. An analysis will also be made to determine if other systems under the ISO’s responsibility also contain similar restricted information and would benefit from additional security precautions.

**Final Report and Recommendations**

A final report will be issued by members of the IRT within 30 days of the occurrence. The report will contain detailed technical information on the break in, conclusions on the extent of the breach, and a summary of all recommendations made to the local ISO, as well as updates on measures already taken. This report will again be distributed to the same personnel who received the initial notifications. It is the responsibility of these groups to determine if further legal or public relations steps must be taken as a result of the compromise.

**Contact Information**

For updated contact information, please refer to the security web page, [https://security.usf.edu](https://security.usf.edu)