## INCIDENT RESPONSE PROCEDURE

<table>
<thead>
<tr>
<th>Code:</th>
<th>ISSP-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td>3.2</td>
</tr>
<tr>
<td>Last Review/Edited:</td>
<td>09/09/2018</td>
</tr>
<tr>
<td>Created by:</td>
<td>Alex Campoe - CISO</td>
</tr>
<tr>
<td>Approved by:</td>
<td>Sidney Fernandes - CIO</td>
</tr>
<tr>
<td>Confidentiality level:</td>
<td>Unrestricted</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Published</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>10/03/2017</td>
<td>Alex Campoe</td>
<td>Total review of the document using new template. Information and link updates.</td>
</tr>
<tr>
<td>3.1</td>
<td>12/01/2017</td>
<td>Alex Campoe</td>
<td>Added Chief Compliance Officer notification.</td>
</tr>
<tr>
<td>3.2</td>
<td>09/09/2018</td>
<td>Campoe</td>
<td>Combined ISSP-002 with ISSP-004, Removal From Network.</td>
</tr>
</tbody>
</table>
Table of contents

ISSP-002 ............................................................................................................................... 1

INCIDENT RESPONSE PROCEDURE .................................................................................. 1

REVISION HISTORY .............................................................................................................. 2

PURPOSE, SCOPE AND USERS .......................................................................................... 4

INCIDENT MANAGEMENT .................................................................................................... 4

1.1. RECEIPT AND CLASSIFICATION OF SECURITY EVENTS, INCIDENTS AND BREACHES ......................................................... 4
1.2. TREATMENT PROCESS FOR SECURITY EVENTS OR INCIDENTS ................................................................................................. 5
1.3. TREATING MINOR INCIDENTS (INSIGNIFICANT OR LOW IMPACT) .......................................................................................... 5
1.4. TREATING MAJOR INCIDENTS (MEDIUM, HIGH, OR SEVERE IMPACT) .................................................................................... 6
1.5. ROLES AND RESPONSIBILITIES ....................................................................................... 6
1.6. LEARNING FROM INCIDENTS .......................................................................................... 8
1.7. DISCIPLINARY ACTIONS .................................................................................................. 8
1.8. COLLECTION OF EVIDENCE ........................................................................................... 8

VALIDITY AND DOCUMENT MANAGEMENT .................................................................... ERROR! BOOKMARK NOT DEFINED.
1. Purpose, scope and users

The purpose of this document is to ensure quick detection of security events and weaknesses, and quick reaction and response to security incidents.

The University of South Florida is a System of higher education composed of multiple campuses and separately accredited institutions located in Tampa, St. Petersburg, and Sarasota-Manatee. Regional campuses and separately accredited institutions may have unique characteristics. Students, faculty, and staff must check with their individual campuses and apply System-wide policies and procedures in conjunction and consistent with the characteristics and guidelines applicable to those campuses.

This policy applies to all IT resources, persons, entities, and personal devices connected to the USF System network or resources, including but not limited to the hardware, software, and USF System institutional data used in these environments.

Individual University areas, including clinical healthcare or clinical research, may create additional policies that build on this and may contain even more stringent controls. Users of this document are all employees of the University of South Florida System, as well as all abovementioned persons.

2. Incident management

An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security related, not those caused by natural disasters, power failures, etc.

An information security incident is a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (ISO/IEC 27000:2009).

A breach is an incident wherein information is stolen or altered in a system without the knowledge or authorization of the system’s owner.

It is important to note that not all incidents are breaches, and the response level for each event varies considerably.

1.1. Receipt and classification of security events, incidents and breaches

Each employee, supplier or other third party who is in contact with information and/or systems of the USF System must report any technology-related event which could lead to a possible incident by sending
an email to security@usf.edu or by contacting IT Help Desk at (813) 974-1222. All such reports will be escalated to the Office of Information Security for evaluation.

Potential breaches, incidents, and events must be reported as soon as possible, by phone or over email.

<table>
<thead>
<tr>
<th>IMPACT LEVEL</th>
<th>Financial Impact</th>
<th>User Impact</th>
<th>Brand Impact</th>
<th>Media Impact</th>
<th>Regulator Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe</td>
<td>Severe financial loss affecting the entire University System</td>
<td>Complete failure of service across the University &gt; or = 5 minutes</td>
<td>University name becomes a byword for misconduct or misadventure</td>
<td>International, long-term media coverage</td>
<td>One or more department shut down, or executives face personal legal liability</td>
</tr>
<tr>
<td>High</td>
<td>Moderate financial loss affecting the entire University System</td>
<td>Failure (partial or complete) of service across multiple departments &lt; 5 minutes, or complete failure across a department &gt; or = 1 day</td>
<td>Loss of multiple high-value donors or introduction of widespread negative brand sentiment</td>
<td>International, short-term media coverage, or national long-term media coverage</td>
<td>Regulator issues notice to comply under penalty of termination (grants, federal/state funds, contracts)</td>
</tr>
<tr>
<td>Medium</td>
<td>Negative budget requiring budget adjustment across multiple departments</td>
<td>Partial local service disruption for &gt; or = 1 day, or total local service disruption in a single department for &gt; or = 1 hour</td>
<td>Loss of one high-value donor or multiple midlevel donors or introduction of short-term negative brand sentiment</td>
<td>National short-term media coverage</td>
<td>Regulator issues an enforceable undertaking</td>
</tr>
<tr>
<td>Low</td>
<td>Negative budget requiring budget adjustment within single department</td>
<td>Partial local service disruption &lt; 1 day, or total local disruption &lt; 1 hour, or attributable rise in daily call center load &gt; or = 20%</td>
<td>Loss of multiple low-value donors or reinforcement of existing negative brand sentiment</td>
<td>Local, long-term media coverage</td>
<td>Regulator requires regular reporting until resolution</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Financial loss within annual budget allowance</td>
<td>Insignificant service disruption, or attributable rise in daily call center load &lt; 20%</td>
<td>Insignificant donor loss</td>
<td>No media coverage or local short-term coverage</td>
<td>No regulator interest; report to regulator is optional</td>
</tr>
</tbody>
</table>

**Figure 1- Impact Level**

### 1.2. Treatment process for security events or incidents

The Office of Information Security employee who received the information about a security weakness or event analyzes the information, establishes the cause and, if necessary, suggests preventive and corrective action. Additional IT resources and personnel are called in as Subject Matter Experts (SMEs) as needed.

### 1.3. Treating minor incidents (Insignificant or Low Impact)
If a minor incident was reported, the Office of Information Security person who received the report must take the following steps:

1. take measures to contain the incident
2. analyze the cause of the incident
3. take corrective actions to eliminate the cause of the incident
4. inform persons who were involved in the incident, as well as the Director of Security Operations, about the incident treatment process

The person who received information about a minor incident must log the incident through the appropriate Help Desk application, with the knowledge that security incidents are to be restricted to a need-to-know basis.

1.4. Treating major incidents (Medium, High, or Severe Impact)

In the case of major incidents, the response should follow the steps outlined on Figure 2, cycling through the stages of Detection & Analysis, Response & Recovery, and Post Incident.

<table>
<thead>
<tr>
<th>Detection &amp; Analysis</th>
<th>Response &amp; Recovery</th>
<th>Post Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>Escalation and Declaration</td>
<td>Containment, Investigation and Eradication</td>
</tr>
<tr>
<td>Analyse Logs and Information Security Events</td>
<td>Validate Incident Scale and Consequence</td>
<td>Based on priority, assemble IRT and notify appropriate parties and escalate incidents.</td>
</tr>
<tr>
<td>Identify potential information security incidents</td>
<td>Assign impact level ratings</td>
<td>Perform incident containment, investigation and root cause analysis, forensics and evidence management</td>
</tr>
<tr>
<td>Categorize incident</td>
<td>Review &amp; confirm ratings</td>
<td></td>
</tr>
<tr>
<td>Endorse ratings</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2- NIST Incident Lifecycle

The Office of Information Security has the obligation and authority to evaluate the seriousness and immediacy of any threat to the campus network and to take action to mitigate that threat. The action taken will be responsible and prudent based on the risk associated with that threat and the potential

---

negative impact to the campus mission caused by making the offending computer(s) inaccessible. Examples of threats that are serious enough to invoke these procedures are:

- The level of network activity is sufficiently large as to cause serious degradation in the performance of the network;
- System administrative privileges have been acquired by someone not authorized;
- An attack on another computer or network has been launched;
- Confidential, private or proprietary electronic information or communications are being collected from the network;
- Required virus protection software is not installed and/or up to date;
- Continued complaints have been received regarding inappropriate activity and no response has been received from the departmental contact regarding the incident.

1.5. Local Threat Vectors

If the potential impact to the campus network or its computers is considered Medium, High, or Severe, and the source of the threat is a local computer attached to the USF network, the computer(s) posing the threat will be blocked immediately. Every attempt will be made to notify the department as the block is put in place. If a block has been put in place it will not be removed until both the department and security personnel agree that the problem causing the incident has been sufficiently addressed.

1.6. Recourse

If a department or individual user feels that a computer has been inappropriately blocked it may request a review of the decision by the University’s Information Security Manager. An appeal of that decision can be made to the Information Security Workgroup.

1.7. Additional Roles and Responsibilities

Figure 3 specifies the roles and responsibilities for each activity related to the response to a major security incident.
1.8. Learning from incidents

The CISO must review all minor incidents every three months, and enter recurring ones, or those which may turn into major incidents on the next occasion, in the Incident Log.

The Director of Security Operations must analyze each incident recorded in the Incident Log (identifying type, relatedness, and cost of incident) and, if necessary, suggest preventive or corrective action.

1.9. Disciplinary actions

Users found culpable of causing a security incident may be subject to disciplinary or corrective actions based upon the policies, rules, regulations and procedures of the University of South Florida System. These actions may include sanctions including, but not limited to, revocation of the employee or student privileges up to and including termination of employment or expulsion. Certain violations, misuse, unauthorized access, or disclosures of confidential information may include civil and/or criminal penalties.

1.10. Collection of evidence

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, an external hard drive, and a flash drive, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime.
If collection of digital evidence is necessary, the Chief Information Security Officer, in conjunction with the Office of the General Counsel, will define how to identify, collect and preserve evidence that will be accepted as evidence in legal and other proceedings, following best practices for such a task.

3. References