# Incident Response Policy

| | | | |
|---|---|---|---|
| Applies To: | All | Policy Number: | ITS-0034 |
| Issued By: | AVP for IT | Policy Version Number: | 1.0 |
| Date Issued: | July 1, 2016 | Last Review Date: | July 1, 2016 |
| | | Last Revised Date: | July 1, 2016 |

**Organizational Details**
The Information Security Incident Response Team (ISIRT) is to promote a computing environment which ensures the confidentiality, availability, and integrity of the University's data and systems. ISIRT will handle all information security incident analysis and response for systems managed by Information Technology Services (ITS), and will offer to assist with any information security incidents on systems within the University network that are not managed by ITS. ISIRT will investigate reports of violations of ITS policies. ISIRT will strive to consistently provide quality service in a timely fashion.

**ISIRT Response Team**
The ISIRT may include all persons accessing and using computing, networking, telephony and information resources through any facility of the University. These persons include students, faculty, staff, persons retained to perform University work, and any other person extended access and use privileges by the University given the availability of these resources and services, and in accordance with University contractual agreements and obligations.

The team will be headed by the AVP for IT, or his or her designee and will be assembled on a case-by-case basis. The Director of Enterprise Applications, Senior Network Manager and Senior Systems Administrator will make the core of the team. Other relevant participants will be invited.

The team may engage key members of the University to aid in the handling of the incident. This will likely include the Senior Attorney, AVP for Human Resources, AVP for Marketing & Public Affairs and the Director of Public Safety.

**Authority**
When a security incident has been declared, the ISIRT team takes on the ownership and responsibility of the incident handling process. This can include directing key members of ITS staff on incident handling decisions and taking the necessary actions to remediate the issue without first discussing it with affected constituents. This includes the possibility of taking temporary action to mitigate a threat posed against the entire network by a segment of the network that is not managed by ITS. Any actions taken without previous discussion will be discussed with affected constituents after the issue has been mitigated. The ISIRT will maintain open lines of communication with the affected constituents during the incident handling process.

**Code of Conduct**
All members of the ISIRT are expected to be familiar with and follow all ISIRT policies. A copy of all ISIRT policies will be provided when an individual joins ISIRT. Proposed revisions to ISIRT policies will be provided to all ISIRT members for comments, and approved updates to any policies will be provided to all current ISIRT members.

All ISIRT members are expected to perform ISIRT tasks to the best of their ability. All ISIRT members are expected to communicate ISIRT information only with individuals who have a need to know, and who have access to the information based on its classification. When communicating ISIRT matters, all ISIRT members are expected to be constructive, to communicate with an appropriate level of technical detail based on the audience, and to project a professional image. ISIRT members should not hesitate to say that they "do not know the answer" if that is the case. ISIRT members will refer any inquiries from media representatives to Marketing & Public Affairs (MPA) instead of providing an answer.

If a member of ISIRT discovers activities that are believed to violate local, state, or federal laws, they should bring the activities to the attention of the ISIRT lead. The ISIRT lead will work with the AVP for IT and the Senior Attorney's Office to facilitate engagement with the appropriate law enforcement agency.

**Information Classification and Disclosure**
All information received by ISIRT is initially shared only within ISIRT. Once the information is properly classified, it may be possible to share the information with a wider audience.

Information received by ISIRT can be classified as one of two types of data:

- Sensitive
- Non-sensitive

Sensitive information is information that will only be shared with ISIRT, the ITS Leadership Team, Senior Attorney's Office, Human Resources and any individuals designated by the ITS Leadership Team. Any information which can easily be tied back to an individual is classified as Sensitive. In keeping with existing policies, a user's right to privacy must be respected as much as possible even when they are suspected of violating policies. Sensitive materials may be reclassified if identifying information has been sanitized. Any materials which contain Protected data or Sensitive data, as defined under the Protected Data and the Sensitive Data Identification Policy, will be treated as Sensitive by ISIRT.

Non-sensitive information is information that can be shared with individuals within ITS as needed. Non-sensitive information is not easily tied back to an individual. Non-sensitive information typically includes IP addresses, timestamps, and similar technical information. Non-sensitive information can be shared with other groups as metrics concerning the incidents and trending information. Non-sensitive information may be shared with any individuals within ITS and any system administrators within the University community who need to know about the incident.

Data is classified by the ISIRT member who initially receives it. If an item is classified as Non-sensitive, any ISIRT member can change the classification to Sensitive. If an item is classified as Sensitive, only the ISIRT lead can change the classification to Non-sensitive. If a member of the ISIRT is unsure of the classification assigned to a particular piece of information, they should assume that the information has been classified as Sensitive.

## Information Requests

Various external groups may request information from ISIRT. The requestor and the type of information requested will determine if the information may be released, and what steps need to be followed to release the information.

*Requests from Internet Services Providers (ISPs), Incident Response Teams (IRTs), and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)*

ISPs, IRTs, and REN-ISAC may contact ISIRT with technical information regarding possible incidents. Any messages of this nature should be forwarded to the ISIRT lead. The ISIRT lead will determine the appropriate response. The ISIRT lead may designate a member of the team to serve as the primary point of contact for communications concerning a particular incident, but all communications should carbon copy the ISIRT lead.

*Requests from Law Enforcement*

All responses to requests for information made by law enforcement must be approved by the Senior Attorney's Office. The only exception to this is if a subpoena or a warrant is issued to ITS or the ISIRT. The warrant or subpoena must be honored; however immediate contact to the Senior Attorney's Office must be made.

*Requests from the University Community*

Requests from non-ITS groups, within the University, for additional information will need to be approved by the AVP for IT and may be subject to sanitizing before the information is released.

*Requests from the Media and External Entities*

All responses to requests for information made by members of the media must be approved by Marketing & Public Affairs (MPA).

If approached by a member of the media for a quote, ISIRT members should only reply with "no comment" and direct the media representative to contact MPA.

Information requests from outside of the University community will be evaluated individually and handled by MPA.

## Human Errors

During a security incident, there is the possibility that an ISIRT member will make a mistake. The emphasis should be placed on correcting the mistake when it is detected, and working to improve the procedures to prevent similar mistakes after the incident has been resolved.

If any member of ISIRT believes that they identified a possible mistake in the investigation, all members of ISIRT who are working on the issue should be notified of the perceived mistake, why it is believed to be a mistake, and what effect this may have on the incident response.

After the incident has been resolved, the ISIRT members involved in the incident will meet to determine what factors led to the mistake. This is not an attempt to assign blame, but rather an attempt to refine the incident response process to prevent similar mistakes in the future.

If an ISIRT member repeatedly makes the same or similar mistakes across a number of incidents, the ISIRT lead may ask the ISIRT member to resign their membership in the ISIRT.

If the mistake constitutes a violation of a University policy, the disciplinary procedure from that policy may apply. If that is the case, the ISIRT lead will be available to speak on the ISIRT member's behalf, if needed.

**Incident Handling**
ISIRT serves a supporting role for Human Resources, Senior Attorney's Office, Student Affairs, and other departments. Requests from departments not specifically identified previously must be authorized by Human Resources or the Senior Attorney's Office. ISIRT will perform technical investigations at the request of these departments, while appropriately respecting the privacy rights of all individuals involved. This can include accessing electronic and voice mail, in accordance with the ITS Policies and Guidelines.

The first step in the incident handling process begins when an event is detected by or reported to ISIRT. The ISIRT lead will evaluate the event and determine if the Incident Response (IR) is appropriate. If the Incident Response is enabled, all the authority granted within this plan will be granted to the ISIRT and a security incident will be declared. Logging of the incident begins, and the incident is triaged in accordance with the procedures defined within.

If the ISIRT lead is unavailable during the time of the event, the ISIRT's backup, or any member of the ISIRT team, may declare a security incident and enable Incident Response after an evaluation of the event. The ISIRT team member that has escalated the incident will become the ISIRT lead for the duration of the incident. At the time the ISIRT lead becomes available, he or she may decide to transition the ISIRT lead role.

Incidents will be brought to the attention of the ITS Leadership Team when they are first classified. All incidents will be detailed in a report that is sent to the ITS Leadership Team.

**Incident Procedures**
Whenever an incident is detected, the following steps will be taken:

1. Identify affected resources: The ISIRT will work to identify the scope of the incident. In this case, the scope involves evaluating the event, or events, identifying what resources might be affected, how many resources are affected, if any services are unavailable as a result of the incident, if any sensitive information might have been accessed and similar information that will be collected and analyzed. As the investigation progresses, the scope may be modified as appropriate.
2. Begin documentation of the incident: The ISIRT assigns each incident a unique incident number. Incident numbers are generated by combining the four digits of the current fiscal year with a four digit counter. So the first incident of 2015 would be 2015-0001, the next would be 2015-0002, etc. All steps taken by the ISIRT lead from this point forward will be documented. After the incident has been resolved, all of the available documentation will be collected for a final report (step #10). Documentation includes a brief description of any actions taken, along with the time that action was taken. This is especially important if the actions are being taken on a resource which may be compromised.
3. Assess incident: An assessment of the impact of the incident will be done. This impact will be brought to the attention of the ITS Leadership Team.
4. Assign responsible ISIRT members: Based on the affected resources and the impact, ITS members with the appropriate knowledge will be assigned to the incident to aid the ISIRT team.
5. Contain the incident: If specific steps are available to contain the incident, the ISIRT will consider the consequences of those actions. If the benefits outweigh the costs, the containment steps will be performed. ISIRT has the authority to take necessary actions to mediate the issue without first discussing it with affected constituents.
6. Collect evidence: The ISIRT will collect evidence of how the incident occurred on the affected resources. Any digital evidence, such as log files and suspicious files, will be preserved by the ISIRT. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. So the first piece of evidence in the first case of 2015 would be 2015-0001-0001, the second piece would be 2015-0001-0002, etc. All collected digital evidence will be documented. This information will be logged in the case file.

7. Determine vulnerability: The ISIRT will work to determine how the incident occurred. If vulnerability is found on the resource, the ISIRT will determine if a patch or workaround is available.
8. Determine malicious actions taken: The ISIRT will work to determine what malicious actions may have been performed on the resource. Determining what actions might have been taken will influence the recommended recovery steps. Depending on the incident, forensic analysis may be required to determine what actions were taken on the resource.
9. Provide recovery steps and take recovery actions: ISIRT is empowered to take the necessary steps to secure the resource and bring it back online. The resource will not be allowed back onto the network until it has been secured. Depending on the extent of the compromise, it may be necessary to restore the resource from tape backup or to rebuild the resource from scratch.
10. Create final report: The ISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports will be provided to the ITS Leadership Team.
11. Archive evidence and report: The ISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the ISIRT section of the ITS safe and a copy will be stored at the University off-site storage location.
12. Process improvement: The ISIRT will work to ensure that the same vulnerability is not present on other University systems. The ISIRT will also work to identify any elements of the Incident Handling process that require improvement.

**History and Updates**
July 1, 2016: Initial Policy