1 DOCUMENT CLASSIFICATION
This document is classified Level 1- Public. The document may be shared internally and/or externally and is published online at http://getprotected.asu.edu/files/incident.pdf

2 PURPOSE
This standard outlines the workflow, roles and responsibilities, and escalation provisions with respect to identifying and handling information security incidents at Arizona State University. A correct, complete, and consistent response is essential to ensure the protection of critical information and systems as well as University compliance with applicable laws, rules, and regulations. Timely and relevant communication with the appropriate parties is necessary to ensure the quality of the response, support legal action if necessary, and maintain public confidence. Complete, accurate documentation and subsequent debriefing are important to prevent the recurrence of similar incidents.

Concerns regarding information security can arise for many reasons. An information security situation that potentially poses a significant risk or could cause significant impact to University systems, assets or personnel would be classified as an incident. An incident, per the National Institute of Standards and Technology (NIST) Computer Incident Handling Guide, is defined as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” A situation that does not appear to be a significant security threat would be classified as an event (see sections 5.1 & 5.2 for more information).

It is the responsibility of all ASU faculty, staff, and students to report information security concerns to the Information Security Office. To report an event or incident, contact the ASU Help Desk at 1-855-278-5080. To report concerns that are not time sensitive or do not require an immediate response, please email infosec@asu.edu or visit http://getprotected.asu.edu.

3 GOALS
The goals of an incident response plan are to:

- Confirm the situation
- Identify the affected systems and devices
- Preserve the integrity of the university computing and network environment and protect university assets and data from further harm
- Restore systems and services to normal operations
- Estimate the potential impact on affected systems and devices
- Preserve and provide evidence to support legal proceedings
- Keep management informed of the situation and response
- Improve security and processes to prevent future incidents

4 SCOPE
This standard applies to all networking, computing, and data devices, both personally owned or university owned devices, attached to the ASU network and/or involved in storage or delivery of ASU data. It addresses violations of ASU’s Computing, Internet, and Electronic Communications Policy (ACD 125) and Information Security Policy. Information security incidents are handled according to this standard and in a manner consistent with applicable laws and regulations. The University may follow a different process than that set forth in this standard if it is determined that it is appropriate to do so under the particular circumstances. Such a decision will be made by the Chief Information Officer in coordination with other appropriate ASU leadership. Laws and regulations that apply include but are not limited to:

- Federal Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Gramm-Leach-Bliley Act (GLBA)
- State Security Breach/Notification Laws (ARS § 44-7501)
- Payment Card Industry Data Security Standard (PCI DSS)
5 WORKFLOW

The chart below identifies the incident response cycle. Each stage of the cycle is described in this section with further detail following in the rest of the standard.
5.1 Identification

Potential information security issues are identified by the Information Security Office using information from a variety of sources including, but not limited to:

- Contact from affected or impacted parties
- Contact from system owners
- Contact from external parties
- User alerts and/or Service Desk requests

Upon discovery of an issue, the party making the discovery shall contact the Information Security Office for consultation. The Information Security Office will determine the scope and confirm the level of data exposed or assets affected or threatened.

Detailed information on sensitive data and data handling can be found in the Data Handling Standard at [http://getprotected.asu.edu/files/data.pdf](http://getprotected.asu.edu/files/data.pdf)

5.1.1 Personally Identifiable Information

During the incident identification process, the University evaluates the potential exposure of sensitive Personally Identifiable Information (PII). A data exposure involving sensitive PII means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable:

- The individual’s social security number.
- The individual’s number on a driver license issued pursuant to §28-3166 or number on a non-operating identification license issued pursuant to §28-3165.
- The individual’s financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual’s financial account.

Sensitive PII also means any information relating to or about any specific individual or groups of individuals protected from disclosure under the Family Educational Rights and Privacy Act of 1974 (FERPA) or the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or any other applicable Federal, State or local statute, law, rule or regulation.

5.1.2 Roles and Responsibilities

It is the responsibility of all users of the ASU network or computing resources, including all ASU faculty, staff, and students, to report information security concerns to the Information Security Office.

System Owner/Administrators

Department technical personnel responsible for systems involved or affected in an incident play an active role in incident discovery and reporting. Department technical personnel will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the Information Security Office or other Incident Response Team members throughout the investigation.

Data Stewards

Data stewards responsible for personally identifiable information play an active role in incident discovery and reporting; data stewards also serve as liaisons with third party service providers and/or other business partners with which the University shares personally identifiable information.
Data stewards must report any suspected or confirmed incident, or third-party notification of an incident, to the Information Security Office immediately upon discovery. The Information Security Office will notify the Privacy Officer and appropriate data stewards.

The data steward will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the Privacy Officer, Information Security Office, Office of General Counsel, or other Incident Response Team members throughout the investigation.

**Managers**

Managers are responsible for ensuring that all employees in their unit are aware of ASU’s policies and procedures for protecting personally identifiable information. Managers must notify the Information Security Office at infosec@asu.edu in the event of a suspected or confirmed exposure.

**Deans, Department Heads, and Senior Leadership**

ASU leadership is responsible for ensuring that all employees in their unit are aware of ASU’s policies and procedures for protecting personally identifiable information. In order for ASU to most effectively respond to information security concerns ASU leadership must notify the Information Security Office at infosec@asu.edu in the event of a suspected or confirmed exposure. ASU leadership may be called upon to elevate priorities within their respective department to resolve an incident efficiently.

### 5.2 Assessment & Classification

When an information security issue has been identified, the Information Security Office (ISO) and the Chief Information Security Officer (CISO) will analyze the situation and determine whether to classify the issue as an event or an incident. All events are investigated and assessed, but only some become classified as security incidents.

When the situation does not appear to be a significant security threat, meaning there is little or no perceived risk to the University community or assets, the ISO will classify the reported issue as an event. The ISO will provide information and instructions for the reporting group to follow.

When the situation potentially poses a significant risk or could cause significant impact to University systems, assets or personnel, the ISO will classify the reported issue as an incident.

The following are examples of information security incidents:

- Denial of Service attack on or originating from Arizona State University controlled systems
- Malicious Code being propagated, controlled or otherwise used to disrupt normal network activity
- Unauthorized access to sensitive information
- Inappropriate usage of University resources

The ISO will work with the Chief Information Officer (CIO) and ASU’s executive leadership, as appropriate, to determine the severity of the incident.

### 5.3 Determine Incident Severity

The ISO will evaluate the scope and potential harm from each incident. Incident severity is based on whether an incident may pose a threat to University resources, stakeholders, and/or services. The determination may include, but is not limited to, the following factors:
• Does the incident involve unauthorized disclosure of high-risk or confidential information?
• Does the incident involve serious legal issues?
• Does the incident cause serious disruption to critical services?
• Does the incident involve active threats?
• How widespread is the incident?

Depending on the severity of the incident (Low, Medium, or High), the CISO will work with the CIO and ASU's executive leadership, as appropriate, to identify appropriate members for the Incident Response Team. An incident severity level of High can only be declared by the CIO and will be based on the recommendation of the CISO and other factors. **When the declaration of an incident's severity is High, the Provost and the CFO will be contacted immediately.**

### 5.3.1 Convene an Incident Response Team

An Incident Response Team is established to provide a quick, effective and orderly response to information security incidents when invoked at the discretion of the ISO. The Incident Response Team's mission is to minimize loss of public confidence, information assets, and/or University revenue. Additional departments and/or individuals may be involved as needed at the discretion of the ISO, including the entities identified in section 5.1.3 and other departments or individuals deemed necessary on a case-by-case basis.

The Incident Response Team, under the guidance of the ISO, is authorized to take appropriate steps deemed necessary to contain, mitigate, and/or resolve information security incidents. The Team is responsible for investigating suspected incidents and reporting findings to management and the appropriate authorities as necessary. The ISO will coordinate these investigations with a named individual on incident response team from the Office of the Provost and the Office of the Chief Financial Officer. Depending on the nature of the incident, the Incident Response Team will likely include representatives from additional University units including:

- College / Department Leadership
- Office of General Counsel
- HIPAA Privacy & HIPAA Security Officers
- Office of Human Resources
- Information Security Office
- ASU Police Department
- Office of the Provost
- Office of the Chief Financial Officer
- Office of Public Affairs
- Student Affairs
- University Technology Office

While isolated incidents may be resolved with minimal involvement outside the initial response team, some incidents may require escalation to notify appropriate entities, to obtain investigative information or assistance, and/or to ensure an appropriate public response by the University. The Incident Response Team may undertake initial and department level escalation as the case indicates. University level and external escalation are recommended by the ISO and confirmed by the CIO, executive leadership, and others as appropriate.

Depending on the nature of the incident, the ISO may be required to work with law enforcement. If served with a warrant or subpoena for information related to security incidents, the ISO will consult with the Office of General Counsel to ensure compliance with federal and state regulations.
5.4 Containment & Eradication

Once an information security incident has been positively identified, the ISO will work with appropriate personnel to isolate the affected equipment, if necessary, in order to prevent secondary threats, attacks on other internal systems, and potential legal liability. A compromised system that is actively causing widespread problems or affecting non-ASU networks or computers will be blocked from the network immediately. Additional immediate actions may include removal from service and/or forensic analysis as appropriate.

On receiving notice of an incident from the ISO, the party responsible for the affected system (e.g., System Owner/Administrators, as defined in Section 5.1.2) is responsible for resolving the issue. This may include reformatting media, reinstalling software, and/or any other steps necessary to prevent similar compromises. Guidelines for securing systems can be found on the ISO’s Web site at http://getprotected.asu.edu. It should be noted that the responsible staff must provide spare hard drives matching the size of the disks of devices in question for imaging and analysis to take place.

The ISO will create a log entry for the incident and notify affected parties of the incident and containment/response measures taken. Academic department leaders will notify their colleges as needed. Status updates will be provided to the Incident Response Team, ASU executive management and other parties as required.

5.5 System Restoration

Once a blocked system is secured, the responsible party should contact the ISO, which will take appropriate measures to clear it for reconnection to the network. ASU reserves the right to take actions necessary to protect the integrity of the university’s computing and network resources, including denial of connection to the university’s network. Refusal or official non-compliance by the responsible party will be handled on a case-by-case basis.

Individuals and departments involved in the incident and incident response will be tasked, in conjunction with UTO, with creating a list of improvements in the area of occurrence to help prevent future incidents. These recommendations and remediation tactics presented by the Incident Response Team will help to close any other holes in the security of the affected department or users.

During the course of the incident, all significant findings, suggestions and resolutions will be logged and filed into the incident response report. This report will be sent out in full to the team for review and final approval during the follow up stages of an incident response.

ASU complies with federal and state requirements to notify individuals if their personal and/or private information has been compromised. The following are examples of incidents that may require notification:

- An authorized user has obtained unauthorized access to PII maintained in paper or electronic form.
- An intruder has compromised systems that store PII.
- University equipment has been used for storage of and/or access to unauthorized data (e.g., pirated music, movies, or software).
- Computer equipment or electronic storage media containing PII has been lost or stolen.
- A department has not properly disposed of storage media containing PII.
- A third party service provider has experienced any of the incidents above with respect to University data that includes PII.

Notification may not be required in incidents in which the University can reasonably conclude that misuse of the compromised information is unlikely and appropriate measures are taken to
safeguard the interests of affected parties. The following are examples of incidents that may not require notification:

- The University recovers stolen equipment and/or storage media, and reasonably concludes that the recovery took place before the information could have been copied, misused, or transferred to another party.
- The University determines that media containing PII was disposed of improperly, but can establish that the information was not retrieved or used without authorization; the University then destroys the media properly.
- Information accessed without authorization contained only directory information (i.e., individuals' names and addresses).
- The data resident on lost or stolen computer equipment or electronic storage media was encrypted and could not be accessed without a secure token or similar device.

6 RESOURCES

ASU Computer, Internet, and Electronic Communications Policy (ACD 125)
http://www.asu.edu/aad/manuals/acd/acd125.html

ASU Information Security Policy
http://getprotected.asu.edu/files/Securitypolicy.pdf

ASU Data Handling Standard
http://getprotected.asu.edu/files/data.pdf

National Institute of Standards and Technology (NIST)
SP 800-61: Computer Security Incident Handling Guide

Revision Request
Your feedback is valued. Anyone who uses this document is invited to use this form to submit suggestions for changes or corrections. Please email infosec@asu.edu or mail to:

UTO Information Security Office
Arizona State University
PO Box 876312
Tempe, AZ  85287-6312