This standard formalizes the requirements for reporting and responding to information security incidents. It serves to minimize the negative consequences of incidents and to improve the University’s ability to promptly restore operations affected by such incidents. It ensures incidents are promptly reported to the appropriate officials, that they are consistently and adequately responded to, and that serious incidents are properly monitored.

The Information Security Policy authorizes the UISO to secure university resources that are actively threatened. When possible, the UISO will abide by this standard and the Incident Response Plan to mitigate the threat. In an urgent situation requiring immediate action and leaving no time for collaboration, the UISO is authorized under the Policy to disconnect any affected device from the network, and to assess vulnerabilities and verify safeguards of university resources.

Definitions
All italicized terms used but not defined in this standard are defined in the Information Security Terms Guideline.

An incident is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy (including the Acceptable Use of Computers and Networks Policy). Examples of incidents include (but are not limited to):

- Unauthorized access of systems or data
- Inappropriate usage of systems or data
- Unauthorized change to computer or software
- Loss or theft of equipment used to store personal information or confidential university data
- Unwanted disruption or denial of service
- Interference with the intended use of university resources
- Compromised user account

While this definition covers numerous potential and actual incidents, the requirement for central incident reporting is aimed at serious incidents as defined below.

A serious incident is an incident that may pose a threat to university resources, stakeholders, and/or services. Specifically, an incident is designated as serious if it meets one or more of the following criteria:

- Involves potential unauthorized disclosure, modification or destruction of personal information (as defined below)
- Involves serious legal issues
- Causes severe disruption to critical services
- Involves active threats
- Is widespread, that is, extends beyond a single unit
- Is likely to raise public interest
Personal information is defined as a person’s first name or first initial and last name in combination with any one or more of the following data elements:

- The person’s Social Security Number
- The person’s Arizona driver license number or non-operating identification license
- The person’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 person’s financial account

Roles and Responsibilities
University-related persons have the following primary roles and responsibilities in connection with incidents:

1. Users of University Resources
   - Promptly report actual or suspected incidents to a local support provider.
   - If the local support provider is unavailable, unwilling or unable to correct an incident, disconnect any affected device’s network connection (the Ethernet cable but not the power supply) and report the incident to the 24/7 IT Support Center, UITS Security Operations or the Information Security Office. See “Contacts” below. In addition, if the incident involves –
     - suspected unauthorized access, theft of university computing equipment or information, or another possible crime, also report the incident to the University of Arizona Police Department (see “Contacts” below) and to local authorities if it occurred away from the main campus.
     - Personally identifiable health information or human subject research information, also report it to the HIPAA Privacy Officer (see “Contacts” below).
     - payment cardholder data, also promptly report it to FSO - Bursar Department Services (see “Contacts” below).
     - a serious incident, report it to unit management and to UITS Security Operations or the Information Security Office (see “Contacts” below).
   - Assist various parties to resolve the incident and help improve practices and prevent or minimize the occurrence of such incidents in the future.
   - In the course of reporting, tracking, and responding to an incident, protect and keep confidential any confidential university data or personal information.

2. Local Support Provider
   - Promptly report all serious incidents reported to or identified by the local support provider to UITS Security Operations or the Information Security Office. See “Contacts” below. In addition, if the incident involves –
     - suspected unauthorized access, theft of university computing equipment or information, or another possible crime, also report the incident to the University of Arizona Police Department (see “Contacts” below) and to local authorities if it occurred away from the main campus.
     - personally identifiable health information or human subject research information, also report it to the HIPAA Privacy Officer (see “Contacts” below).
     - payment cardholder data, also report it promptly to FSO - Bursar Department Services (see “Contacts” below).
- a serious incident, report it to unit management and to UITS Security Operations or the Information Security Office (see “Contacts” below).

- Evaluate and respond to incidents on a timely basis to prevent additional loss of or harm to university resources, in accordance with University and unit policies and procedures, including the Incident Response Plan and the Incident Handling Guideline.

- Assist various parties to resolve the incident and help improve practices and prevent or minimize the occurrence of such incidents in the future.

- Following initial reporting and upon performing remedial actions for any serious incident, notify the Information Security Office or UITS Security Operations for accurate closure of the problem report. See “Contacts” below.

- Notify the affected user of remedial steps taken and recommended mitigating activities.

- In the course of reporting, tracking, and responding to an incident, protect and keep confidential any confidential university information or personal information.

3. Information Security Liaisons
   • Participate in and support establishment of incident response processes, including incident reporting.

   • Maintain a problem report or other documentation of the incident.
   • Attempt to contact the user or local support provider regarding any discovered or reported incident.
   • Communicate to the user and the local support provider any actions that need to be taken by them, the reasons for them, the steps required to re-establish service and any relevant technical information about the incident.
   • If the user or local support provider is unavailable, unable or unwilling to correct the incident expeditiously, take necessary and appropriate actions to mitigate or remediate in accordance with University and unit policies and procedures, including the Incident Response Plan and the Incident Handling Guideline.
   • Initiate escalation procedures to the appropriate office or party as necessary.
   • In the course of reporting, tracking, and responding to an incident, protect and keep confidential any confidential university information or personal information.

5. UISO
   • Coordinate investigation of serious incidents.
   • Report serious incidents to the Chief Information Officer.
   • Activate a Virtual Security Incident Response Team, as deemed necessary.
   • Convene an ad hoc committee to review any serious incident involving possible acquisition of personal information that may result in breach notification pursuant to Arizona Revised Statutes Section 44-7501 (Notification of breach of security system), or possible unauthorized acquisition, access, use or disclosure of personally identifiable health information that may result in breach notification under.
   • Report findings of fact relevant to the serious incident to the ad hoc committee, if any.
   • If a decision is made to notify affected subjects, report the information required by ABOR Policy 9-202 to the President, the Vice President for Legal Affairs and General Counsel, and the Vice President for External Relations, then to the Executive Director of the Arizona Board of Regents.
• Initiate escalation procedures to the appropriate office or party as necessary.
• If a decision is made to notify affected subjects, coordinate the drafting of notification communications with management of the affected unit, approve final version (with any other appropriate party), and ensure that the notification procedures are executed.
• If a decision is made that notification is not required, notify the Chief Information Security Officer.

6. **Ad Hoc Committee**
• Review any serious incident that potentially involves unauthorized access to and acquisition of personal information that may result in breach notification pursuant to Arizona Revised Statutes Section 44-7501 (Notification of breach of security system).
• Determine, based on findings of fact by the UISO, whether criteria for notification under law or University policy have been met and, if so, determine the means of notification.
• Recommend action based on its deliberations and findings.
• Report findings and recommendations to the President and the Chief Information Officer.

7. **Management of Affected Unit**
• If advised by the UISO that the ad hoc committee has recommended action, issue notification communications without unnecessary delay, subject to the needs of law enforcement, in coordination with the UISO.

8. **HIPAA Privacy Officer**
• Inform the Information Security Office of reported serious incidents. See “Contacts” below.
• Investigate any reported incident involving personally identifiable health information or human subject research information.
• If a decision is made to notify affected subjects of an incident involving personally identifiable health information, coordinate the drafting of notification communications with management of the affected unit, approve final version (with any other appropriate party), and ensure that the notification procedures are executed.

9. **FSO – Bursar Department Services**
• Inform the Information Security Office of reported serious incidents. See “Contacts” below.
• Initiate escalation procedures to the University’s acquiring bank, member bank and card company, as necessary.

10. **University of Arizona Police Department**
• Inform the Information Security Office of any reported loss or theft involving confidential university information or personal information. See “Contacts” below.

**Contacts**
• [Security Incident Reporting Web Form](#)
• 24/7 IT Support Center – [support@email.arizona.edu](mailto:support@email.arizona.edu) or 626-TECH
• Information Security Office and UISO –[infosec@email.arizona.edu](mailto:infosec@email.arizona.edu) or 621-UISO
• UITS Security Operations – [secops@arizona.edu](mailto:secops@arizona.edu)
• HIPAA Privacy Officer –621-1465
• University of Arizona Police Department – 621-UAPD
- Financial Services Office/ Bursar Department Services: merchants@fso.arizona.edu or 621-5781

Related Guidance
- Information Security Policy (IS-100)
- Exceptions Procedure (IS-P100)
- Information Security Terms Guideline (IS-G100)
- Incident Response Plan (IS-P1100)
- Incident Handling Guideline (IS-G1100)
- 16 CFR Part 314, Standards for Safeguarding Customer Information [Section 501(b) of the Gramm-Leach-Bliley Act]
- Health Insurance Portability and Accountability Act 45 CFR Parts 160, 162, and 164 (HIPAA)
- ABOR Policy 9-202 (University Responsibilities)
- Acceptable Use of Computers and Networks (IS-701)
- American Recovery and Reinvestment Act of 2009, P.L. 111.5, Section 13402
- Arizona Revised Statutes Section 44-7501 (Notification of breach of security system)
- Payment Card Industry Data Security Standard Requirement 12.9

Revision History

<table>
<thead>
<tr>
<th>Revision Type</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>11/12/08</td>
</tr>
<tr>
<td>UA-ISAC Review</td>
<td>4/2/09</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/09</td>
</tr>
</tbody>
</table>