Purpose

All authorized users have an interest in the security of university resources at The University of Arizona, and share in the responsibility for protection of those resources, prevention of problems, and incident detection and response. The purpose of this plan is to describe the general procedures that will be followed in response to those incidents involving university resource that rise to the level of serious incidents. A serious incident is 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) that may pose a threat to University resources, stakeholders, and/or services. Specifically, an incident is a serious incident 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

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

Virtual Security Incident Response Team

Serious incidents will be responded to by a specially-formed team of individuals from across the University, the Virtual Security Incident Response Team (VSIRT). This team will be comprised of technical resources with the appropriate skills to identify, assess, respond to and communicate the effects of serious incidents. VSIRT members will be designated by the UISO, who is authorized under the Information Security Policy to act in the best interest of the University to secure university resources that are actively threatened and to abide by the incident handling procedures to mitigate the threat. Full cooperation with the VSIRT is required of all authorized users of university resources.
Response to Serious Incidents

Generally speaking, serious incidents will be responded to by containing and eradicating the threat or cause of the problem as soon as possible and as completely as possible while investigative and corrective actions are taken. In addition, appropriate measures to support investigation of the incident will be taken. Cooperation of authorized users with these steps is required. Specifically, procedures will include the practices described in Appendix A to this plan, as appropriate.

Related Guidance

Arizona Revised Statutes Section 44-7501 (Notification of breach of security system)
ABOR Policy 9-202
16 CFR Part 314, Standards for Safeguarding Customer Information [Section 501(b) of the Gramm-Leach-Bliley Act]
Payment Card Industry Data Security Standard Requirement 12.9
Information Security Policy (IS-100)
Acceptable Use of Computers and Networks (IS-702)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)
Incident Response Standard (IS-S1100)
Incident Handling Guideline (IS-G1100)

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>11/15/08</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>
Appendix A

Response Plan for Serious Incidents

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

- Involves potential unauthorized disclosure, modification and destruction of personal information
- 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

Serious Incident

Is it a serious incident?

Yes

Execute response strategy based on Incident Response Standard and Incident Handling Guideline

No

Notify UISO

Was there a possible crime?

Yes

Involve law enforcement

No

Was VSIRT needed?

Yes

Activate VSIRT

No

Execute response strategy based on Incident Response Standard and Incident Handling Guideline

Was there a potential unauthorized acquisition of personal information?

Yes

Convene ad hoc committee

No

Notify Chief Information Officer

Notification of subjects required?

Yes

Report to President, VP for Legal Affairs & General Counsel, VP for External Relations

No

Report to unit management

Include:
- Registrar if FERPA
- FSO Bursar’s Dept. if Payment Card Numbers
- External Relations if Reputational Risk
- Human Resources if HR Data

Coordinate notification with unit management

Is it a serious incident?

Yes

No