THE UNIVERSITY OF ARIZONA

Guideline Title: Information System Activity Review
Guideline Number: IS-G603
Responsible Office: Office of Information Security

PURPOSE:
The purpose of the Information Security Activity Review Guideline is to ensure the regular review of information system security activity, such as audit logs, access reports, and security incident tracking reports. Resources that must be considered are people, facilities, processes, hardware, software, networks, and data.

Information Security Activity Review covers all units, especially those that interact with Confidential University Data or data that is covered by information security regulatory or contractual requirements.

REQUIREMENTS:
Each unit will take reasonable and appropriate steps to ensure that university resources have the appropriate hardware, software, or procedural auditing mechanisms installed on them to enable review of information system activity on a periodic basis. The unit’s risk assessment shall determine the level and type of auditing mechanisms that will be implemented.

The following are auditable events for information systems, where logs/reports should be generated:
- Failed authentication attempts
- Information system start-up or shutdown
- Use of privileged accounts (e.g., system administrator account)
- Creation of new privileged accounts
- Escalation of privileges on existing accounts
- Security incidents

The unit’s designee shall review logs/reports of information system activity implemented on University resources on a scheduled and periodic basis.

Findings from the risk assessment shall be used to help determine the frequency of scheduled reviews; each unit should review the system security activity on a periodic basis.

The following factors should be considered with respect to the frequency of both scheduled and periodic reviews of system activities:
- The sensitivity of data on the University resources
- The criticality of the University resources
- The importance of the applications operating on the information systems
- The degree to which the information systems are connected to other University resources and the degree to which that connection poses a risk to sensitive or Confidential University Data
- Regulatory and contractual requirements shall determine the length of time that each unit is required to retain its system activity review records.

The information system security activity review process shall include:
- Definition of what activity is significant
- Procedures for defining how significant activity will be identified and, if appropriate, reported
- Procedures for maintaining the integrity of records of significant activity
- Identification of which workforce members will review records of activity
- Definition of which activity records need to be archived and for what duration

If an anomaly is discovered during monitoring of audit logs, or if a system alert is sent to the log monitor, the following steps must be taken:

- Assess whether or not a potential vulnerability has indeed been found by reviewing the audit log
- If a vulnerability is found, determine the root cause of the vulnerability
- Assess whether or not data, particularly sensitive data, may have been accessed.
- If data was accessed, immediately report this finding to the Information Security Office. The Information Security Office will determine if an incident response investigation is warranted.
- Remediate the vulnerability and test to ensure that the vulnerability has been corrected.
- Document the reported vulnerability and the required remediation steps.
- Share the remediation documentation with the Information Security Office.

**Related Guidance**
- Information Security Policy (IS-100)
- Information Security Terms Guideline (IS-G100)
- Incident Response Standard (IS-S1100)
- Incident Response Procedure (IS-P1100)
- Incident Handling Guideline (IS-G1100)

All *italicized terms* used in this standard are defined in the Information Security Terms Guideline (IS-G100).

**Revision History**

<table>
<thead>
<tr>
<th>Initial Draft</th>
<th>4/16/12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date</td>
<td>11/5/12</td>
</tr>
</tbody>
</table>