Purpose and Summary
This standard supports ISO-1100 Information System Audit, Accountability, and Activity Review Policy and applies to any Information Resource that stores, processes, or transmits University Information classified as Confidential or Regulated, as defined in the University's Data Classification and Handling Standard, and Enterprise Systems. Additionally, all classifications of University Information must be protected in proportion to their security risk.

This standard also establishes requirements for the following:
1. The responsible person for ensuring log events are captured and logs monitored
2. Log collection and aggregation systems
3. Log collection and retention
4. Logging and monitoring related data that must be provided to the Information Security Office
## Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise System</td>
<td>Any Information System, whether provided through a vendor or through local IT, which: (a) supports business processes that span units; (b) is universally, or nearly universally, used by one or more classes of users (e.g. employees, students, researchers, faculty, etc.); (c) can be considered to be an official or de facto 'system-of-record' for the institution; and/or (d) is a dependency for a system that meets one of the previous criteria.</td>
</tr>
<tr>
<td>Information Resources</td>
<td>University Information and related resources, such as equipment, devices, software, and other information technology.</td>
</tr>
<tr>
<td>Information System</td>
<td>A major application or general support system for storing, possessing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>The individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to the owned Information Systems on behalf of the University and is responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.</td>
</tr>
<tr>
<td>ISO</td>
<td>The University's Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.</td>
</tr>
<tr>
<td>Unit</td>
<td>A college, department, school, program, research center, business service center, or other operating Unit of the University.</td>
</tr>
<tr>
<td>University Information</td>
<td>Any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.</td>
</tr>
</tbody>
</table>
Statements of Standard

A. All classifications of University Information must be protected in proportion to their information security risk.

B. Information System Owners with responsibility for Information Systems that store, process, or transmit University Information classified as Confidential or Regulated, as defined in the University’s Data Classification and Handling Standard, and/or an Enterprise System must:
   1. Ensure log events are captured and reviewed regularly.
   2. Follow a written procedure per type of log for defining alert criteria, report criteria, and defining a significant event.
   3. Use a log collection and aggregation system to automatically capture log events and generate alerts and reports. The log collection and aggregation system must meet these minimum requirements:
      a) Alerts must be generated and sent to the Information System Owner for review. Events will be generated at least once per week.
      b) Reports must be generated and sent to the Information System Owner for review. Reports will be generated at least once per week.
      c) Alerts and reports generated by the log collection and aggregation system must be kept for 6 years from the date the alert or report is generated.
      d) Significant events in the log collection and aggregation system must be kept for six (6) years from the date they are generated.
      e) Logged events in the log collection and aggregation system must be kept for one (1) year from the date they are generated.
      f) Access to events in the log collection and aggregation system, reports, and alerts must be limited based on principle of least privilege.
      g) Validation checks must be performed to verify that logged events are not modified once they are in the log collection and aggregation system.
      h) Access to the log collection and aggregation system must be recorded and reported.
      i) Logged events in the log collection and aggregation system must be encrypted at rest.
   4. Investigate alerts generated by the log collection and aggregation system and escalate to the Information Security Office (ISO) upon discovery if the Information System Owner believes there is a need for ISO review. The following information must be sent along with the alert when escalating:
      a) Date and time of activity
      b) Origin of activity by IP address or hostname
      c) Identification of user, service, or process performing the activity
      d) Description of the attempted or completed activity
   5. Log the following types of events:
      a) Privileged account usage
      b) Information system resource start-up or stop
      c) Failed authentication attempts
      d) General login activity
      e) Password change activity
      f) Data modification and access, where training is required to access the data or where required for regulatory compliance
g) Reports on training status of users, where required for accessing systems or data

6. Collect the following meta-data per event:
   a) Date and time of activity
   b) Origin of activity by IP address or hostname
   c) Identification of user, service, or process performing the activity
   d) Description of the attempted or completed activity

7. Provide the following data to the Information Security Office:
   a) Reports and alerts generated by the log collection and aggregation system including:
      i. date and time of the activity
      ii. origin of activity by IP address or hostname
      iii. identification of user, service, or process performing the activity
      iv. description of the attempted or completed activity
   b) Amount of data in bytes sent to the log collection and aggregation system by source per day.
   c) Amount of data in events sent to the log collection and aggregation system by source per day.

Related Documentation/Resources

- University of Arizona Information System Audit, Accountability, and Activity Review Policy
- ISO Exception Process/Procedure
- Data Classification and Handling Standard