SandBox Union

SandBox Union, LLC

SECURITY AUDIT, MONITORING, AND LOGGING POLICY

BACKGROUND

This policy is intended to facilitate the effective implementation of the processes necessary to meet security audit best practices. This policy directs that SandBox Union meet these requirements for all sensitive IT systems.

STATEMENT OF POLICY

SandBox Union will conduct security audits for all systems classified as sensitive. Each system will be audited for security controls once every three years at a minimum to assess whether IT security controls implemented to mitigate risks are adequate and effective.

AUDITABLE EVENTS

All SandBox Union IT systems must, at a minimum, be capable of and configured to:

1. Produce audit logs with the necessary event information, and
2. Have the ability to offload audit log data to a log aggregation server.

The Director of Infrastructure and Information Security determines, based on a risk assessment and mission/business needs, that the IT system is auditing the following events:

1. Authentication attempts;
2. Authenticated individual;
3. Access time;
4. Source of access;
5. Durations of access; and
6. Actions executed.

Network devices such as routers, switches, hubs, firewalls, and other devices that facilitate the transfer of packets from one point to another must be configured to log security data as well as errors. Applications, including web services and database services, residing on servers that utilize cached or separate authentication capabilities must also maintain logs of all security, application, and event-related information. Events should be logged in real-time, to the fullest extent possible, stored locally, and sent to the central log analysis server as the event is recorded. Network devices must also be configured to transmit recorded events to the central log analysis server as the event is recorded by the network device.

End-user workstations, including but not limited to desktops and laptops, must also maintain logs of security-related events. These devices must also forward the security event information to the central log analysis server as the event occurs.

CONTENT OF AUDIT RECORDS

The Director of Infrastructure and Information Security will configure the system such that the audit records contain sufficient information to, at a minimum:

1. Establish what type of event occurred (i.e., event id);
2. When (date and time) the event occurred (i.e., timestamp);
3. Where the event occurred (i.e., destination IP address);
4. The outcome (success or failure) of the event;
5. The identity of any user/subject associated with the event (i.e., user id/process id); and
6. File names involved and access control or flow control rules invoked.

SandBox Union will centrally manage the content of audit records generated by all servers providing application support to the agency, including but not limited to database servers, messaging servers, file servers, print servers, middleware servers, and DNS servers.

SandBox Union will centrally manage the content of audit records generated by all network devices providing connectivity to the agency, including but not limited to routers, firewalls, IDS/IPS, and VoIP servers.

AUDIT STORAGE CAPACITY

The Director of Infrastructure and Information Security will ensure audit storage capacity is allocated according to system configuration to prevent exceeding capacity.

RESPONSE TO AUDIT PROCESSING FAILURES

The Director of Infrastructure and Information Security will configure systems. All systems classified as sensitive will be configured by the Director of Infrastructure and Information Security to provide real-time alerts when the following audit failure events occur:

1. Recording of authentication attempts and/or
2. Escalation of privileges.

These events will be considered a potential security event.

AUDIT REVIEW, ANALYSIS, AND REPORTING

The Director of Infrastructure and Information Security will review and analyze information system audit records at least every 30 days for indications of inappropriate or unusual activity and report findings.

The Director of Infrastructure and Information Security will adjust the level of audit review, analysis, and reporting within the information system when there is a change in risk to SandBox Union's operations, assets, individuals, or other agencies.

If the system is classified as sensitive, audit review, analysis, and reporting processes must be integrated to support organizational processes for investigation and response to suspicious activities. This integrated approach correlates records across different repositories to gain agency-wide situational awareness. Further integration of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information should be used to enhance the ability to identify inappropriate or unusual activity.

The Director of Infrastructure and Information Security is responsible for monitoring the infrastructure and log files on a continuous basis and documenting the activity. The Director of Infrastructure and Information Security must analyze SIEM information.

TIME STAMPS

The system must be configured to generate time stamps to include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

PROTECTION OF AUDIT INFORMATION

Audit records, audit settings, and audit reports must be protected from unauthorized access, modification, and deletion.

Access to audit information must be restricted to the Director of Infrastructure and Information Security and those authorized to perform security audits and/or investigate security incidents. Audit information must not be accessible by end-users of the resource or any other non-system/system administrator.

Regular backup and archival processes must be in place for audit files in order to protect historical log data and collect new log data processed by the server.

The central log analysis server must be heavily protected as it will contain sensitive data pertaining to all SandBox Union systems. To provide this protection, the central log analysis server must be located on a dedicated network segment and not on the internal network. The central log analysis server will forward alerts about anomalous events to the security operations staff for review and action.

Audit records must be backed up at least once every twenty-four hours to a different system or media than the system being audited.

AUDIT RECORD RETENTION

SandBox Union will retain audit records consistent with SandBox Union's Document Retention and Destruction Policy to provide support for after-the-fact investigations of security incidents and to meet regulatory information retention requirements.