SACSF/G15.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 15.0: Logging and Monitoring

Purpose

Cyber security is fundamental to the successful operations of the Government of South Australia (SA). The South Australian Cyber Security Framework (SACSF) and supporting guidelines have been prepared to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of SA Government agencies.

This guideline has been developed to assist agencies and applicable suppliers to understand and implement the event logging and monitoring requirements of the SACSF. This guideline should be applied to all event logs, security logs, and audit logs generated by the systems, networks, and infrastructure that operate, transmit, and store SA Government information and data.

Scope

The SACSF applies to:

- SA Government public sector agencies, that is, administrative units, bodies corporate, statutory authorities and instrumentalities of the Crown as defined in the *Public Sector Act 2009*.
- Suppliers to the SA Government and non-government personnel who provide services to agencies.

The SACSF policy statements related to this guideline are:

- SACSF Policy Statement 2.6: Robust ICT Systems and Operations – Standard operating procedures and technical controls must be in place to provide a consistent and secure approach to system administration, maintenance and configuration activities.

Event logging and monitoring requirements in the SACSF (for tier two agencies and above):

- An event logging strategy is developed and implemented covering events to be logged, logging facilities to be used, event log retention periods and how event logs will be protected.
- A centralised logging facility is implemented, and systems are configured to save event logs to the centralised logging facility as soon as possible after each event occurs.
- An accurate time source is established and used consistently across systems and network devices to assist with the correlation of events.

Guidelines

The following capabilities should be considered for implementing logging and monitoring controls for security events:

- standards and procedures
- log sources
- time synchronisation
- log content
- log retention
- log protection
- monitoring of security events
- threat intelligence
- continuous improvement
- third party requirements.

Definitions, detailed recommendations and examples of implementation are outlined in the following sections.

Definitions

Log type	Information types
Event logs Event logs encompass a range of logs that capture various activities and events occurring within a system or network. Event logs provide a comprehensive record of different types of events, both security-related and non-security-related (general IT operations), such as system performance, operational issues, and changes.	• system startup and shutdown events • application launches and terminations • file modifications and access • system and application errors • network communication events • user account changes • system configuration changes • hardware or software component failures.
Security logs Security logs are a subset of logs that specifically capture events and activities related to security incident, threats, or vulnerabilities. Security logs should be used to identify and investigate security incidents, detect unauthorised access attempts, and understand the overall security posture.	• failed login attempts • successful login events • access control changes • network traffic anomalies • malware detections • security policies violations • intrusion attempts • suspicious system or application behaviour.
Audit logs Audit logs refer to logs that capture records of actions, activities and changes, serving as evidence of accountability, integrity and transparency. Audit logs provide a detailed record of events that can be audited and reviewed for incident response, compliance and forensic investigation purposes.	• user authentication and authorisation events • privileged user activities • administrative changes • configuration modification • data access and manipulation events • compliance-related events • system and application activities relevant to regulatory standards.

Guidelines

Standards and procedures

- Agencies should develop and maintain documentation at the strategic level and operating level to address security requirements for logging and monitoring controls.
- Documentation should include a Logging and Monitoring Standard that outlines:
    - security objectives
    - roles and responsibilities
    - compliance requirements
    - retention requirements
    - privacy statements
    - information classification
    - log format and patterns
    - backups
    - capacity management
    - encryption requirements
    - time synchronisation
    - third party contractual requirements.
- Procedure documents should also be developed, which include detailed instructions on how to implement and carry out logging and monitoring activities on a day-to-day basis to ensure the consistency, accuracy and effectiveness in logging and monitoring practices. The following are examples of logging and monitoring procedures:
    - Log collection procedure – specify the systems, applications, and devices from which logs should be collected and provide step-by-step instructions on how to configure logging settings.
    - Log retention and storage procedure – define the duration for logs to be retained and specify the storage location for the logs, including redundancy, backup copies.
    - Log analysis and monitoring procedure – outline the process of monitoring logs in real-time or on a scheduled basis. Specify the use of security tools or platforms for log analysis, such as security information and event management (SIEM) system or log analysis software.

Log sources

- Most systems generate events to record actions performed by users of the system or the system itself. Agencies should identify the log sources that are critical to business operations and security management, which may include[1]:
  - operating systems
  - databases
  - web applications
  - server applications
  - user applications
  - email servers
  - system access
  - domain name system (DNS) services
  - remote access services
  - mobile devices
  - multi-function devices
  - gateways
  - web proxies
  - firewalls
  - data loss prevention
  - privileged access management
  - other security solutions.
- Agencies should ensure all relevant log sources (including the log sources managed by third parties) in scope are configured to generate logs based on agency security requirements.
- The onboarding of new log sources should be undertaken through agency's standard change management processes. An agency should follow the defined logging and monitoring standard and procedures to configure log settings for the log sources.

[1] The Information Security Manual maintains a list of logs that can be used to detect and investigate cyber security incidents: Guidelines for Cyber Security Incidents | Cyber.gov.au.

Time synchronisation	• An accurate, standard, and consistent time source is important to enable the correlation and analysis of security-related events and other recorded data, and to support investigations into security incidents. Agencies should establish and synchronise the standard time sources across systems and network devices to assist with event logs. • Domain joined devices should be configured to source their time from domain controllers. • Non-domain joined devices should be configured to source their time from core switching infrastructure. • Third party managed systems and cloud services should be configured to standard time sources based on agreements between the agency and service providers.

Log content	• Agencies should specify the required information to be included in the logs, such as:
	  ○ date and time of the event (timestamps)
	  ○ relevant user or process (user ID, process ID)
	  ○ relevant filename
	  ○ event description and activities
	  ○ source or destination addresses (IP, MAC, port numbers) and the devices involved.

Log retention	• Agencies should determine the appropriate retention period for logs based on legal, regulatory[2], and business requirements. Agencies should consider retaining logs for an extended period in case of investigation or incident response needs. • The retention requirements should be documented in the agency's standard and the agreements with third party service providers.
Log protection	• Agencies should define measures to protect log files from unauthorised access, modification, or deletion. • Agencies should ensure that logs are stored in a secure location and storage with restricted access control. • Agencies should back up the logs and consider redundancy on logging facilities to ensure the logs are available during system downtime and disruptions.

[2] Refer to the State Records Act 1997, Standard – Managing digital records in systems, Standard – Minimum recordkeeping metadata requirements, General Disposal Schedules.

Monitoring of security events	• Agencies should implement real-time monitoring capability for security events, using intrusion detection systems, intrusion prevention systems, next generation firewalls, SIEM systems, and other security solutions to actively monitor event logs and identify potential security incidents. • Agencies should implement a centralised logging facility and automate the event analysis, triage and incident response processes, using SIEM and security orchestration, automation and response solutions. Log sources should be configured to save event logs to the centralised logging facility as soon as possible after each event occurs. • Agencies should establish alerting mechanisms to promptly notify key stakeholders and impacted users when critical security events and/or anomalies occur. Escalation procedures and communication plans should be defined and documented for prompt incident response.
Threat intelligence	• Agencies should integrate threat intelligence feeds into the logging and monitoring systems to enhance the detection of known threats and indicators of compromise (IOCs). • Intelligence feeds include open-source threat intelligence, commercial threat intelligence providers, government sources, and security research communities. • Log patterns should be leveraged during proactive threat hunting exercises. By searching for known malicious log patterns and/or IOCs, agencies should identify potential threats that might have passed traditional security safeguards.
Continuous improvement	• Logging and monitoring controls should not be treated as a one-time setup - they require ongoing attention and maintenance to remain effective. • Agencies should define a process for regular reviews and audits of logging and monitoring capabilities to identify opportunities for improvement, such as fine-tuning alerting thresholds, expanding log sources, or integrating additional security tools.
Third party requirements	• For consistency of security practices and compliance, agencies should define the contractual requirements for third parties that manage agency's systems and logs, based on the agency's logging and monitoring standard and scope of services. • Considerations should include the retention of logs, security of logs, access to logs by the state, and the return or destruction of logs at the end of the contract. • Agencies should document logging requirements in the service level agreements or contracts with third parties.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this guideline. There is no specific impact on Aboriginal people.

Related documents

- South Australian Cyber Security Framework (SACSF)
- South Australian Protective Security Framework (SAPSF)
- Premier and Cabinet Circular PC 004 – ICT, Digital and Cyber Security Requirements (PDF 359 KB)
- Australian Government Information Security Manual
- Australian Signals Directorate Windows Event Logging and Forwarding (PDF 1.1 MB)
- Essential Eight Maturity Model

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Chief Information Security Officer	
Division: Office of the Chief Information Officer	Compliance: Optional
Review number: V1.0 DRAFT	Original approval: 10 April 2024
Next review date:	Latest approval: