IT Security Standard – Logging and Monitoring

Version	Approved by	Approval date	Effective date	Next review date

Standard Statement			
Purpose	The detection of potential or actual information security incidents relies on timely and comprehensive event information being available from key security controls. These events are critical during forensic investigation in the event of a security incident. This standard sets out the baseline requirements for logging and monitoring security events within UNSW.		
Scope	This standard applies to all: • Network, compute and storage devices that attach to UNSW networks or connect to UNSW IT systems and applications, including those owned or operated by third-parties and contractors. • All login and logout by individuals to the UNSW network.		
Are Local Documents on this subject permitted?	☐ Yes	☐ Yes, subject to any areas specifically restricted within this Document	☐ No
Standard			

1. Controls

1.1 Information security event collection and logging

1.1.1 UNSW collects log data relating to activity and security events on network, compute and storage devices including IT Systems and applications. The type of events recorded (see Control 2.3.1) must be defined based on the capability of the system producing log data, and the classification of information stored within the system (Data Classification Standard).

1.2 Sources of security event logs

1.2.1 Key systems creating and aggregating security logs, including Internet and intranet boundary devices such as routers, firewalls, IDS/IPS, Authentication Servers, Content filters and DNS must have functionality to create information security events upon detection of unwanted activity, and send these events to a centralised collection point. Examples of security event logs that should be captured (but not limited too) include:

- Traffic blocked by a firewall due to policy restriction.
- Traffic detected as anomalous, malicious or fake by an intrusion detection or anti-virus protection system.
- Successful, failed and released network connection attempts, for example from DHCP or radius services.
- HTTP logs from an external proxy or web services.

- Email or web browsing sessions that do not meet UNSW policy.
- Authentication or privileged escalation success and failure on device management interfaces, business applications and databases.
- Web, database and application service errors, failures and timeouts.
- Access, copy and modification of private, payment or other sensitive information.
- Backup process event start and end time as well as failures.
- Changes to database schemas and file system permissions.

1.3 Security event minimum log standards

1.3.1 Whilst the type of event logs that can be logged is reliant on the capability of the log source, security event logs must aim to record:

a) The date and time of the activity being logged.

b) A unique user identifier associated with an activity.

c) The source IP address of the user activity or external event that occurred.

d) The security event that has occurred for example the detection of an attack signature.

e) Activity undertaken, for example logon, logoff, creates, modify, delete or copy.

1.3.2 The device or service producing the security event logs must be configured to send these events to a centralised collection point which resides within a protected environment.

1.4 Protecting security event logs from unauthorised modification or destruction

1.4.1 Security event logs must be protected from unauthorised modification and deletion. This can be achieved by:

a) Ensuring that access to the log source and log destination is securely authenticated (e.g. TACACS for network devices) and restricted (e.g. access only via separate management subnet or separate administrative control).

b) A specialised, logging service that cryptographically signs security event logs to protect the logs from modification. The service must not have a log deletion or purge facility.

c) Restrict access to authorised users based on business need.

1.5 Security event log formats

1.5.1 Where possible, security events must be logged using an industry-standard non-binary format that is human readable. This reduces the possibility of these logs being inaccessible in future and increases UNSW's capability to integrate, centralise and correlate information security events.

1.6 Synchronisation of security event log sources

Synchronisation of event logs timestamps is critical and improves the ease of performing a forensic investigation of actual or suspected security events.

1.6.1 All UNSW IT Network attached equipment must have time synchronised to a known time source so that accurate timing is available across system logs, for example by network time protocol (NTP) synchronisation to a central clock source.

1.7 Security event log retention and rotation

1.7.1 Security logs must be retained for at least two (2) years as UNSW records, or as specified by external legal or regulatory requirements.

1.7.2 The rotation of security logs is system-specific and is determined based on the capability of the device or service producing the logs. However a common technique in security attacks is to produce a high-volume of security events to force security logs to overwrite the

evidence of attack. To reduce the risk of this happening, security logs must be configured to either:

a) Have a maximum size commensurate with one (1) week logging at full logging rate, to minimise the risk of an attack overwriting recent evidence.

b) Notify administrators when log capacity is approaching full at various thresholds, example 25%, 50%, 75% and 100%.

1.8 Monitoring and review of security event logs

1.8.1 UNSW has systems and processes to analyse security event log data to identify suspected and detected breaches in a way that minimises business disruption.

1.8.2 Where possible, log monitoring must be automatic and rule-based, to immediately alert on suspected security events. Automated event monitoring and alerting systems must have the capability to report devices that fail to report, to reduce the risk that a security event goes un-noticed.

1.8.3 Where no automated mechanism exists to alert possible security incidents, key security event logs must be checked frequently for evidence of actual or potential security incidents. Key security event logs include those generated by:

- Border routing devices.
- Network and application firewalls, both internal and external.
- Intrusion detection, anti-virus and malicious code protection services.
- Internet-connected services and systems such as web servers, load balancers and proxy services used in the delivery of web applications that are available on the Internet.
- Corporate authentication and authorisation services.
- Data stores containing private or other confidential information.

1.9 Automated log correlation

Many actual or attempted security attacks are identified only by the correlation of multiple security events that have been raised by disparate sources.

1.9.1 Where possible, UNSW must identify unwanted security scenarios and the indicators of those scenarios, so automated rules can be implemented that correlate disparate logs and alert in the event that the scenario actually happens. This could be achieved through a Security Information and Event Management (SIEM) solution.

2. Control Exceptions

All exemption requests must be reviewed assessed, and approved by the relevant business stakeholder. Please refer to the ISMS Base Document for more detail.

3. ISMS Mapping with Industry Standards

The table below maps the ITSS_06 Logging and Monitoring Standard with the security domains of ISO27001:2013 Security Standard and the Principles of Australian Government Information Security Manual.

ISO27001:2013	Information Security Manual
12 Operations security (12.4 Logging and monitoring)	Access Control (Event Logging and Auditing)

4. Document Review, Approval & History

This section details the initial review, approval and ongoing revision history of the standard. Post initial review the standard will be presented to the ISSG recommending the formal UNSW policy consultation and approval process commence.

A review of this standard will be managed by the Chief Digital Officer on an annual basis.

4.1 Quality Assurance

This document was designed and created by external and internal consultants in consultation with internal key technical subject matter experts, business and academic stakeholders.

4.2 Sign Off

Endorsement	Date
ISSG - Information Security Steering Group	
ITC - Information Technology Committee	
CDO – Chief Digital Officer	

Accountabilities	
Responsible Officer	Chief Digital Officer
Contact Officer	
Supporting Information	
Parent Document (Policy)	IT Security Policy
Supporting Documents	Nil
Related Documents	Data Classification Standard Data Handling Guidelines ISMS Base Document ITSS_02 Data Security Standard
Superseded Documents	Nil
UNSW Statute and / or Regulation	Nil
Relevant State / Federal Legislation	Nil
File Number	2016/16925 [ITSS_06]

Definitions and Acronyms

No terms have been defined

Revision History

Version	Approved by	Approval date	Effective date	Sections modified