Information Security Monitoring Procedure

Reference: NIS DOC C1-01
DocumentKits Issue No: 1.0
DocumentKits Issue Date: 25/08/2021

1. Scope

All Organisation Name's network and information systems are subject to this procedure.

2. Responsibilities

The Information Security Manager performs the risk assessment to identify the type and level of audit logging and monitoring that might be required for each individual information asset.

Owners of individual assets are responsible for identifying and agreeing with the Information Security Manager the logging and monitoring capabilities of the assets they own and for having them configured to meet the requirements of the risk assessment.

<<Content removed for sample purposes>>

<<Content removed for sample purposes>>

3. Audit logging

The
"servers/systems/devices"

for which User activity audit logging is configured,
"and the audit logging software that is deployed"

together with the schedule/matrix of audit log requirements
"and reporting regularity"

are set out
"where? This will need to be specific to your network and information systems and ensure that you capture sufficient useful information to detect security incidents."

SAMPLE

Audit logs are subject to access control.
"Describe the technical configuration of this control."

Audit logs are reviewed
"using a continuous automated monitoring and alerting process/manually every [X] weeks"

for the purposes of identifying irregularities and potential remediation actions.

System administrators are prohibited from erasing or deactivating logs of their own activities
"and the technical configuration of this control is [ ]"

"Audit logs record access to personally identifying information (PII), including by whom, when, the PII principal whose information was accessed, and any changes made. [Describe the technical configuration of this control.]"

"Logs that could contain PII are subject to automatic deidentification or deletion by means of [describe the mechanism you will apply to ensure this occurs in line with your retention schedule]."

The schedule/matrix of audit log requirements and the audit log reports are classified as confidential information and must be handled in line with the requirements of this information security management system (ISMS) for handling confidential information.

The following data protection or privacy protection restrictions also apply:
"specify"

"Logs are reviewed manually each day and by automated processes to ensure near-continuous oversight."

Organisation Name deals with error and fault logging as follows:
"Here you should insert details about how you deal with these issues, applying the guidance of 12.4.1 of ISO 27002."

4. Monitoring system use

The
"servers/systems/devices"

SAMPLE

for which User activity monitoring is configured, together with the schedule/matrix of monitoring requirements
"and reporting regularity"

are set out
"where?"

System administrators are prohibited from erasing or deactivating logs of their own activities
"and the technical configuration of this control is [ ]"

The schedule/matrix of monitoring requirements and the monitoring reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.

The following data protection or privacy protection restrictions also apply:
"specify"

Monitoring reports are reviewed
"define regularity and responsibility."

Any evidence of system misuse is reported to the Information Security Manager, who investigates further, and the disciplinary process may be invoked. See also section D1 of the NIS Manual.

5. Protection of log information

Audit logging is configured as set out above.

System administrators
"and other suitable senior/competent staff?"

are permitted to access audit logs when there is business need to know.

System administrators are prohibited from disabling logging activity; disabling audit logs or tampering with audit log information is treated as a
"serious offence"

in the disciplinary policy and may result in
"immediate dismissal."

SAMPLE

"Describe how system logs and event types are investigated; what tools might be used, etc."

"Describe how system logs are securely stored and archived, bearing in mind that logs may need to be accessible when the rest of the organisation's network and information systems are unavailable."

"Any modifications to log data are performed only on copies of the data rather than the original."

6. Administrator and operator logs

<<Content removed for sample purposes>>

7. Clock synchronisation

The clocks of all information systems within Organisation Name
"are synchronised with (or if necessary specify in a schedule different points of synchronisation for geographically dispersed systems) [specify what and how the synchronisation is performed across the network.]"

Throughout its information systems, the date stamp format used by Organisation Name is:
"dd/mm/yyyy."

The timestamp format used by Organisation Name is
"hhmm applying the 24-hour clock."

The clocks on all servers and all organisational information processing devices
"(including laptops and PDAs)"

are checked on a
"regularity?"

basis
"how?"

and corrected where necessary. The record of completed checks and any necessary corrections is forwarded to the Head of IT (CIO).

SAMPLE

"Where appropriate, information about clock synchronisation in Cloud services used by Organisation Name is requested and, where necessary, checked [define how often checks are made].

Where Organisation Name provides Cloud services to customers, information about clock synchronisation will be made available on request."

8. Reporting

Anomalous behaviour is reported through the incident reporting procedure (Reporting Information Security Weaknesses and Events).

"Describe other reportable log results. This might include log data that influences business objectives or reflect the results of business decisions."

The following governance reporting requirements also apply:
"details"

"**9. Service provider logs**

Logging requirements for services provided by other parties (including Cloud services) are defined below.

Where services or parts of services are provided by other parties, those parties are assigned the following roles:
1.
2.
3.

Only [role(s)] may access logs made available to other parties. The following logs are made available to other parties:
1.
2.
3.

Logs held by other parties are reviewed [using a continuous automated monitoring and alerting process/manually every [X] weeks] for the purposes of identifying irregularities and potential remediation actions.

Where a service provided by other parties stores or processes PII, the logs associated with the service record access to PII, including by whom, when, the PII principal whose information was accessed, and any changes made.

The following data protection or privacy protection restrictions also apply: [ ].

Logs that could contain PII are subject to automatic deidentification or deletion by means of [describe the mechanism you will apply to ensure this occurs in line with your retention schedule].

[List any other requirements that apply to logs associated with services provided by other parties.]"

SAMPLE

"**10. Customer logs**

<<Content removed for sample purposes>>

"**11. Cloud service logs**

<<Content removed for sample purposes>>

Document owner and approval

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the Master List of Document Approval.

SAMPLE