NetGain systems	No of Pages	**1** of **5**
	Document Classification:	Internal
	Effective Date	1 Aug 2025
LOGGING AND MONITORING	Doc No	ISMS-TECH-06
	Revision	1.0

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

This procedure sets out the ways in which the organisation monitors anomalous behaviour in systems and applications, and identifies information security events that can lead to an incident and to support investigations. It should be read in conjunction with document *ISMS-ORG-10 Information Security Event & Incident Management* which sets out how events are assessed and what actions must be taken.

SCOPE

This control applies to systems and applications within the organisation's ICT environment.

The organization does not manage or monitor the office network or shared infrastructure. Network-level monitoring of the office infrastructure is outside the organization's scope. Monitoring efforts are instead focused on cloud-based systems, applications, endpoints, and services managed by the organization.

REFERENCE

ISO/IEC 27001 Standard	Annex A 8.15 Logging Annex A 8.16 Monitoring Annex A 8.17 Clock synchronisation

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

The System Administrator shall monitor information processing systems and the activities of users to identify any actions that are not in keeping with the secure use of the information processing facilities provided.

PROCEDURE

1. Audit Logging

The company shall enable and maintain audit logging capabilities on all cloud platforms, applications, and systems under its control, to ensure traceability of user and system activities, support incident response, and fulfil compliance requirements.

Systems in Scope:

- Cloud-hosted infrastructure
- SaaS platforms and observability/security management tools used in service delivery

- Source code repositories and CI/CD pipelines
- Internal applications and systems related to client services

Events to be logged:

- User authentication events, including all successful and failed login attempts
- Access to sensitive or client-related data, including success/failure
- Changes to configurations, especially related to security controls or audit settings
- Privileged/admin actions, including account modifications and policy changes
- Critical operations within cloud platforms or security/observability systems (e.g., data deletions, service deployments)

Audit logs shall minimally include:

- Username or user ID
- Timestamp of the event
- Source IP or device
- Action performed and outcome (success/failure)
- Affected systems or data

Passwords and sensitive personal data must never be logged. Systems and applications should be configured to mask or exclude sensitive information in audit logs.

Where third-party or cloud platforms limit logging capability, the company shall:

- Enable available logging features (e.g., cloud-native logging tools)
- Document any logging limitations
- Perform a risk assessment and implement compensating controls where possible

2. Monitoring Activities

The company shall implement monitoring activities tailored to its cloud-based architecture and managed systems to support detection and response to security incidents. Scope of monitoring includes:

- Cloud and SaaS infrastructure (e.g., usage anomalies, unauthorized access)
- Observability/security platform logs (e.g., rule changes, alert suppression, suspicious queries)
- Application-level logs for critical services
- Privileged account activity
- Security tool telemetry, such as endpoint protection alerts (where applicable)

The organisation shall investigate and address all security alerts and alarms raised from the different monitoring activities as well as all suspicious activities. The alerts and suspicious activities to be detected shall include, but not limited to the followings:

- Malware or ransomware indicators
- Unauthorized login attempts and brute-force activity
- Unexpected admin actions or privilege escalations
- Web-based attacks (e.g., SQL injection, XSS)
- Unusual access times or data transfer volumes

The security monitoring services shall be fine-tuned to improve its accuracy and minimise false positives on an on-going basis. This includes the creation, modification and customisation of rule sets required for the finetuning.

3. Protection of Log Information

The organisation shall automate the generation of log reports to maintain the integrity of the reports and to make sure that the generated reports are not tempered with. Exception reports shall be generated when requested to facilitate detection of unauthorized activities and access (such as frequent access, privileged admin access, etc.).

Appropriate access control will be put in place to ensure that logged information is only used as intended, protect against modifications and unauthorized access, and prevent such data being used for any other purpose. The said logged information will be deleted or de-identified in the information processing facilities as per defined retention schedule.

Controls such as cryptographic hashing and recording in an append-only and read-only file shall be implemented to protect against unauthorized changes to log information and operational problems with the logging facility. There shall be no capability to modify or delete an audit log or record through the use of system utilities like file update, file-aid, file patch, etc. If there are such attempts, this shall be logged as a security incident.

4. Clock Synchronization

To support accurate event correlation across systems and platforms:

- All systems (cloud instances, VMs, SaaS tools, CI/CD environments) shall synchronize their clocks using a trusted time source (e.g., NTP).
- Time synchronization will be enforced as part of system provisioning scripts or configuration management.