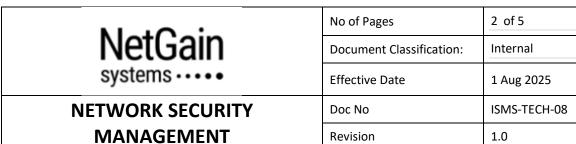
NI 10 °	No of Pages	1 of 5
NetGain systems	Document Classification:	Internal
	Effective Date	1 Aug 2025
NETWORK SECURITY	Doc No	ISMS-TECH-08
MANAGEMENT	Revision	1.0

# **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



# **Contents**

DMENTS LOG	1
	3
ENCE	3
AND RESPONSIBILITIES	3
ROLS	4
METIMORK SECURITY	/
SEGREGATION OF NETWORKS	4
LOGGING AND MONITORING	5
NETWORK CHANGES	5
NETWORK SECURITY INCIDENTS	5
	NETWORK SECURITY  NETWORK SERVICE PROVIDERS.  SEGREGATION OF NETWORKS.  LOGGING AND MONITORING.  NETWORK CHANGES.

N. IO.	No of Pages	3 of 5
NetGain systems	Document Classification:	Internal
	Effective Date	1 Aug 2025
NETWORK SECURITY	Doc No	ISMS-TECH-08
MANAGEMENT	Revision	1.0

## **PURPOSE**

This document defines how the organization protects its cloud-based systems, applications, and remote workforce through secure management of logical networks under its control. It outlines how network security principles are applied to cloud services, remote access, and endpoint connectivity, in order to safeguard the confidentiality, integrity, and availability of systems and data.

## **SCOPE**

This procedure applies to:

- All organization-managed systems and cloud infrastructure (e.g., virtual networks, cloud firewalls, and service-level security controls)
- All remote and endpoint connections to organizational services
- Network configurations within platforms directly controlled by the organization (e.g., VPCs, VPNs)
- Third-party services where the organization defines access or security rules (e.g., SaaS with IP restrictions or federated access)

The organization operates in a shared office environment and does not own or manage the office network or infrastructure (e.g., routers, firewalls, access points). Security of those components is outside the scope of this procedure.

#### REFERENCE

ISO/IEC 27001 standard Annex A 8.20 Networks security

Annex A 8.21 Security of network services Annex A 8.22 Segregation of networks

## **ROLES AND RESPONSIBILITIES**

Traditional Network Administrator roles (e.g., managing routers, switches, LANs) do not apply within the company's shared office model. The following will be the key roles and responsibilities for the execution of this control.

Role	Main Responsibilities
Cloud Administrator	Design and secure virtual networks
	Manage cloud-based firewalls and routing rules
	Implement VPN and endpoint access controls
	Monitor network-level alerts from cloud providers

N. IO.	No of Pages	4 of 5
NetGain systems ·····	Document Classification:	Internal
	Effective Date	1 Aug 2025
NETWORK SECURITY	Doc No	ISMS-TECH-08
MANAGEMENT	Revision	1.0

Role	Main Responsibilities
System Administrator	Configure remote access for team members
	Ensure secure endpoint and authentication configuration
	Ensure secure endpoint and authentication configuration

#### **CONTROLS**

## 1 Network Security

The organization secures its virtual and logical networks in line with cloud security best practices and zero trust principles. The following controls are implemented:

- Cloud network segmentation
- Firewall rules and access control lists (ACLs) to restrict inbound/outbound traffic
- VPN or SSO-based secure remote access for personnel working remotely
- Device-level protection (e.g., endpoint firewalls) for remote users
- Default-deny configurations in cloud platforms to limit unauthorized access
- TLS encryption for all external and internal traffic
- Disabling unused services and ports in virtual environments
- Secure DNS resolution and control over public IP exposure

All configurations are aligned with industry benchmarks such as the CIS Benchmarks for relevant cloud services and systems.

## 2 Network Service Providers

The organization relies on cloud and internet service providers for connectivity. The following apply:

- Security features of cloud network services (e.g., WAF, DDOS protection, network isolation) are assessed and configured based on risk.
- Network access to third-party SaaS applications is secured through:
  - IP allow-listing (where supported)
  - o Enforced SSO and MFA
  - Role-based access controls (RBAC)
- The organization ensures cloud services meet agreed service levels and security expectations, including encryption in transit, secure protocols, and audit capabilities.

## 3 Segregation of Networks

Segmentation is enforced through the following:

Using logical boundaries (e.g., cloud subnets, security groups, containers, access tiers).

NI 10 1	No of Pages	5 of 5
NetGain	Document Classification:	Internal
systems · · · •	Effective Date	1 Aug 2025
NETWORK SECURITY	Doc No	ISMS-TECH-08
MANAGEMENT	Revision	1.0

- Production, development, and testing environments are segregated at the network and accesscontrol level.
- All guest Wi-Fi or office-provided wireless access is treated as untrusted; personnel accessing
  organizational systems must use encrypted tunnels (e.g., VPN, HTTPS).

## 4 Logging and Monitoring

Network activity within organization-controlled environments is logged and monitored using cloud-native tools. These tools detect:

- Unauthorized access attempts
- Unexpected open ports or traffic flows
- Suspicious connections or endpoint behaviour

Alerts are triaged and escalated in accordance with ISMS-ORG-10 Information Security Event and Incident Management.

## 5 Network Changes

All changes to cloud networks or related configurations (e.g., firewall rules, VPN changes) must be handled per *ISMS-TECH-11 Change Management*.

## 6 Network Security Incidents

Any event involving unauthorized access, anomalous network behaviour, or breach of logical boundaries is treated as a security incident. Incidents will be logged and investigated following *ISMS-ORG-10 Information Security Event & Incident Management*.

For critical incidents, isolation and remediation steps are taken (e.g., shutting down affected virtual machines, revoking credentials, modifying firewall rules).