NETWORK CONFIGURATION POLICY

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

**INTERNAL INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

[1. Introduction 4](#_Toc65491980)

[1.1 Document Definition 4](#_Toc65491981)

[1.2 Objective 4](#_Toc65491982)

[1.3 Scope 4](#_Toc65491983)

[1.3.1 Applicability to employees 4](#_Toc65491984)

[1.3.1 Applicability to External Parties 4](#_Toc65491985)

[1.3.2 Applicability to Assets 4](#_Toc65491986)

[1.4 Related Documents / References 4](#_Toc65491987)

[2. Policy Statements 6](#_Toc65491988)

[2.1 Network Connection Control 6](#_Toc65491989)

[2.2 Network Service Levels 6](#_Toc65491990)

[2.3 Segregation of Networks 6](#_Toc65491991)

[2.4 Device Information Protection 6](#_Toc65491992)

[2.5 External Connection Points 6](#_Toc65491993)

[2.6 Network Device Approval 6](#_Toc65491994)

[2.7 Management / Change Control 7](#_Toc65491995)

[2.8 Firewall Protection 7](#_Toc65491996)

[2.9 Traffic Denial by Default 7](#_Toc65491997)

[2.10 Essential / Non-Essential Services 7](#_Toc65491998)

[2.11 Non-Disclosure of Private IPs 7](#_Toc65491999)

[2.12 Routing Updates 7](#_Toc65492000)

[2.13 Network Documentation 8](#_Toc65492001)

[2.14 Wireless Access Points 8](#_Toc65492002)

[2.14.1 Wireless – Prohibited Use 8](#_Toc65492003)

[2.14.2 Wireless – Network Access 8](#_Toc65492004)

[2.14.3 Wireless – Home Access 8](#_Toc65492005)

[2.14.4 Wireless – Public Access 9](#_Toc65492006)

[2.15 Wireless Access & Encryption 9](#_Toc65492007)

[2.16 Wireless Coverage 9](#_Toc65492008)

[2.17 Network Device Logging & Monitoring 9](#_Toc65492009)

[2.18 Configuration Baselines and Review 9](#_Toc65492010)

[2.19 Network Security Baseline 9](#_Toc65492011)

[2.20 Penetration Testing 9](#_Toc65492012)

[2.21 Intrusion Prevention / Intrusion Detection 10](#_Toc65492013)

[2.22 Connection Removal 10](#_Toc65492014)

[2.23 Network Time Synchronisation 10](#_Toc65492015)

[2.24 Proxying 10](#_Toc65492016)

[2.25 Capacity Management 10](#_Toc65492017)

[3. Policy Compliance & Enforcement 11](#_Toc65492018)

[3.1 Compliance Measures 11](#_Toc65492019)

[3.2 Enforcement 12](#_Toc65492020)

[4. Exception Process / Glossary 13](#_Toc65492021)

[4.1 Exception Process 13](#_Toc65492022)

[4.2 Glossary / Acronyms 13](#_Toc65492023)

[5. Document Management 14](#_Toc65492024)

[5.1 Document Revision Log 14](#_Toc65492025)

[5.2 Document Ownership 14](#_Toc65492026)

[5.3 Document Coordinator 14](#_Toc65492027)

[5.4 Document Approvers 14](#_Toc65492028)

[5.5 Document Distribution 14](#_Toc65492029)

# Introduction

## Document Definition

This document is a Policy.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Objective

The objective of this policy is to provide global information security requirements to:

* Ensure that firewalls, wireless access points, and other network devices are effectively configured, secured, and monitored;
* Protect the logical boundaries of XXXX. (XXXX) network and therefore its underlying information assets;
* Design, configure, document, and manage all XXXX networks and network devices.

## Scope

### Applicability to employees

XXXX refers to XXXX.as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Policy applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-004 - Data Classification Policy*
* *XXXX-POL-ALL-009 - Access Control Policy*
* *Risk Management Policy*
* *XXXX-POL-ALL-012 - Incident Response Policy*
* *XXXX-POL-ALL-016 - Cryptography and Key Management Policy*
* *XXXX-STD-ALL-008 - Wireless Access Point Configuration Standard*
* *XXXX-STD-ALL-016 - Logging & Monitoring Standard*
* *XXXX-STD-ALL-019 - Network Time Synchronisation Standard*
* *XXXX-PRC-ALL-002 - Change Control Procedure*
* *XXXX-PRC-ALL-026 - Firewall-**Router Change Request Procedure*
* *XXXX-PRC-ALL-007 - Log Review & Monitoring Procedure*

# Policy Statements

## Network Connection Control

All network connections must be protected through a combination of security controls sufficient for the protection of XXXX Information Data Assets. These must be based on the type and purpose of the connection and include, but are not limited to, network segmentation, deployment of firewalls and other security appliances, and appropriate authentication mechanisms.

Access to information available through the network must be strictly controlled in accordance with the *XXXX-POL-ALL-009 - Access Control Policy* in order to prevent and detect unauthorised access while providing secure access to authorised users and systems.

Security requirements will be addressed in all network services agreements.

## Network Service Levels

Business resilience and continuity minimums required service levels, and appropriate security controls must be identified, defined, and documented for any provider of network services, whether in-house, or outsourced to a third-party provider.

## Segregation of Networks

Networks will be segregated to prevent access overlap and to minimise the impact of any threat to the network.

## Device Information Protection

Any data assets on network devices must be restricted to authorised users in accordance with the *XXXX-POL-ALL-004 - Data Classification Policy*.

## External Connection Points

Connections between the internal network and external networks must be made via approved connection points (e.g. in a DMZ) and only if specifically allowed. A comprehensive record of all connections must be maintained and reviewed at a minimum annually by Information Security.

## Network Device Approval

The implementation of any new networking devices (i.e., routers, switches, firewalls) or components of networking systems must follow the local change management process and be approved by Head IT

## Management / Change Control

Any changes to network devices and corresponding rule-sets / Access Control Lists (ACLs) must follow appropriate change control, testing and authorisation processes as detailed in the *XXXX-PRC-ALL-002 - Change Control Procedure* and *XXXX-PRC-ALL-026 - Firewall-Router Change Request Procedure* respectively.

Primary ownership for management of network devices is the Head of IT

## Firewall Protection

All XXXX networks connected to untrusted networks (i.e. open internet, DMZ, vendors, etc.) must be protected by a firewall (or equivalent) technology capable of stateful packet inspection.

## Traffic Denial by Default

Traffic to or from any untrusted network (including the Internet) into or from any XXXX network must be denied by default.

Required access must be explicitly allowed and be in accordance with the *XXXX-POL-ALL-009 - Access Control Policy*.

## Essential / Non-Essential Services

Network device configuration standards will include a documented list of all services, protocols and ports, including business justification and approval for each.

All non-essential services on network devices must be disabled or removed when possible.

## Non-Disclosure of Private IPs

Private IP addresses and routing information must not be disclosed to any unauthorised party.

Permitted methods include:

* Network Address Translation (NAT);
* Placing servers behind proxy servers / firewalls;
* Removal or filtering of route advertisements for private networks that employ registered addressing;
* Internal use of RFC1918 address space instead of registered addresses.

## Routing Updates

Routers must be protected from inconsistent and/or incorrect routing updates.

## Network Documentation

Network documentation (including network and data flow diagrams) must be created and maintained at a sufficient level of detail and be subjected to a review and management approval by the Head IT

## Wireless Access Points

The implementation of wireless access points must include the necessary segmentation via firewall or router control lists to allow only traffic specifically allowed and must follow proper change management and approval of Head IT

### Wireless – Prohibited Use

* Only wireless devices approved by Head IT shall be used / connected / interfaced with the XXXX network;
* The use of personal wireless access points within XXXX is prohibited;
* The use of wireless devices / technologies / software that interferes with or enumerates wireless infrastructures are prohibited;
* Exposed wireless hardware shall not be moved, disconnected or tampered with.

### Wireless – Network Access

* All wireless infrastructures within XXXX shall be configured in accordance with the relevant *XXXX-STD-ALL-008 - Wireless Access Point Configuration Standard* ;
* Wireless infrastructures shall be managed, supported, installed and maintained by authorised individuals only;
* Only XXXX approved authentication protocols may be used;
* Only XXXX approved encryption ciphers may be used;
* Perimeter firewalls shall be installed between wireless networks and the XXXX data environments, configured to deny or control any traffic from the wireless environment inbound;
* All wireless devices within XXXX shall have strong encryption technology enabled for both authentication and transmission;
* All clients shall be clearly identifiable, and all activity logged in accordance with the *XXXX-PRC-ALL-007 - Log Review & Monitoring Procedure*;
* Physical access to wireless access points, gateways, and handheld devices shall be protected appropriately;
* All XXXX offices shall be subject to an annual wireless scan (or network equivalent) to identify unauthorised wireless networks in accordance with the *XXXX-PRC-ALL-011- Rogue Access Point Detection Procedure*.

### Wireless – Home Access

* Home wireless infrastructure, if used to transmit XXXX data, shall be configured in accordance with the relevant *XXXX-STD-ALL-008 – Wireless Access Point Configuration Standard*;
* Exceptions shall be approved and documented by the XXXX Head IT on an individual basis. Mitigating controls shall be applied and documented.

### Wireless – Public Access

* No XXXX owned devices (which include any device carrying XXXX data) shall be connected to any public wireless infrastructure without the prior approval by the XXXX Head IT on an individual basis.

## Wireless Access & Encryption

Wireless access must be authenticated and encrypted. The encryption solution must comply with *XXXX-POL-ALL-016- Encryption and Key Management Policy*.

## Wireless Coverage

Wireless access must not exceed the desired coverage area.

## Network Device Logging & Monitoring

Systems must log relevant activity. Logs must be reviewed and retained in accordance with *XXXX-STD-ALL-016 - Logging & Monitoring Standard*.

If applicable, the review must be followed by an effective response as detailed in *XXXX-POL-ALL-012 - Incident Response Policy*.

## Configuration Baselines and Review

All network components must be hardened in compliance with documented configuration baselines in line with *XXXX-POL-ALL-017 - System Configuration Policy*. Network devices must be reviewed on an annual basis to verify configuration. The use of an automated tool may support manual reviews.

## Network Security Baseline

Configuration baselines must include a security configuration baseline as a component, or a security configuration baseline must exist separately and be applied to all systems.

Security baselines must take into account all applicable legislative, statutory, regulatory, and contractual requirements and be configured accordingly.

## Penetration Testing

Firewall rule base reviews and penetration tests must be performed periodically based on a risk assessment performed in accordance with *Risk Management Policy*. The use of an automated tool may support manual reviews.

## Intrusion Prevention / Intrusion Detection

An Intrusion Prevention System or Intrusion Detection System must be used to detect unauthorised activity on wireless and wired networks as identified by a Risk Assessment performed in compliance with the *Risk Management Policy*. Results from the intrusion detection system above a pre-defined threshold must be identified and must trigger an alert. Alerts must be followed by an effective response.

## Connection Removal

Network connections must be removed in a timely basis when no longer required.

## Network Time Synchronisation

All XXXX network devices will be configured to receive time synchronisation protocols in accordance with the *XXXX-STD-ALL-019 - Network Time Synchronisation Standard*.

## Proxying

Some form of Internet, spam and/or web proxy filtering must be performed on all connectivity between trusted and untrusted networks, particularly the Internet.

## Capacity Management

The following capacity requirements should be built into al systems from the design phase:

* disk usage and size;
* network traffic load;
* load balancing;
* necessary processing power; and
* necessary memory requirements.

# Policy Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| For a selection of network connections, evidence that connections (Internal and External) are appropriately controlled and approved by management. | * Network diagrams * Network configuration information * Documented approvals (approvals by management for connections (email, security committee meeting notes, etc.) |
| For a selection of network connections to an untrusted network, evidence that the traffic is routed through a firewall | * Network diagrams * Network configuration information |
| For a selection of newly implemented networking devices or components, evidence of approval | * Approval documentation |
| For a selection of network devices, evidence that unnecessary services have been disabled | * Network configuration information * Inquiry with appropriate personnel to determine the required services for each device |
| For a selection of routers, evidence that the routing update protocols are protected and/or updates to the routing table is controlled | * Router configuration information |
| For a selection of network documentation, evidence that the documentation was reviewed and approved | * Physical sign-off on documentation * Email or other electronic workflow tool output |
| For wireless network access, evidence that:   * Access is authenticated * Access is encrypted   The wireless access does not exceed the coverage area | * Wireless access configuration information * Network diagrams * Building floor plans |
| For a selection of network devices , evidence that device logs are configured and reviewed | * Device logs configuration information * Inquiry with appropriate personnel regarding the relevancy of items logged and action taken as a result * Physical sign-off on logs * Email evidence of log review * Trouble-ticketing system or other workflow tool output showing status of follow-up actions (open / closed) |
| For a selection of network devices, evidence that the device configuration was reviewed or that a tool was used to perform configuration review | * Tool output / report * Email or other workflow tool output |
| For the Intrusion Detection System, evidence that   * Networks are monitored by the system   Alerting thresholds are appropriate and follow-up action is taken | * Intrusion Detection System configuration information * Helpdesk system or other workflow tool output showing status of follow-up actions (open/closed) |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| Access Point | A wireless receiver that can connect one or more wireless devices to each other or an existing wired network. |
| DMZ | Demilitarised Zone. |
| Encryption Cipher | An algorithm for performing encryption and decryption. |
| Firewall | A system designed to prevent unauthorised access to or from a private network. |
| Intrusion Detection | An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack. |
| Intrusion Prevention | An intrusion prevention system (IPS) provides policies and rules for network traffic along with an intrusion detection system, but allows an administrator to provide an action upon being alerted. |
| Penetration Test | A series of tests or procedures performed in an attempt to gain unauthorised access or to circumvent security controls. |
| RFC1918 | A standard by which networking equipment assigns IP addresses in a private network. The RFC reserves the following ranges of IP addresses that cannot be routed on the Internet:   * 10.0.0.0 - 10.255.255.255 (10/8 prefix) * 172.16.0.0 - 172.31.255.255 (172.16/12 prefix) * 192.168.0.0 - 192.168.255.255 (192.168/16 prefix) |
| Router | A device that forwards data packets along networks. |
| Stateful Packet Inspection | Only allow connections that are part of an existing communication channel. |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## Document Ownership

This Policy is owned by the YYYY

## Document Coordinator

This Policy is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* IT
* Information Security