Document ID	POL-FW
Version	1.0
Effective Date	March 1, 2026
Owner	Rachel Okafor
Approved By	David Whitfield

Northgate Engineering Ltd

Firewall and Network Security Policy

Information Security Management System

Classification: Internal Use
Northgate Engineering Ltd

Table of Contents

1. Introduction and Purpose

1.1 Introduction

The boundary between the organization's networks and untrusted networks, including the internet, is one of the most frequently probed points in any environment. Firewalls and network security controls determine what traffic may cross that boundary and what may move between internal zones, and they are the first line of defense against opportunistic, internet-based attack.

A firewall protects only to the extent that it is correctly configured, maintained, and reviewed. A device left with default settings, permissive rules, or unmanaged change quickly becomes a liability rather than a control. This policy establishes how the organization configures and manages firewalls and network security so that the boundary is protected by design and remains so over time.

1.2 Purpose

The purpose of this policy is to ensure that every device within scope is protected by a correctly configured boundary firewall or equivalent network control, that traffic is permitted only where there is a justified business need, and that firewall and network configuration is controlled, documented, and reviewed.

This policy supports protection against unauthorized access from untrusted networks and limits the ability of an attacker to move within the organization's networks once a foothold is gained.

1.3 Policy Statement

The organization shall ensure that all in-scope devices are protected by a boundary firewall or equivalent network protection, that inbound and outbound access is restricted to that which is justified and approved, and that firewall and network configuration is securely managed, documented, and reviewed. Default and unnecessary access shall be denied.

2. Scope

2.1 Organizational Scope

This policy applies across the whole organization and to all business functions that operate, administer, or depend on firewalls, network devices, and the boundary between trusted and untrusted networks. It applies to systems and services the organization operates directly and to those operated by third parties or cloud providers on the organization's behalf.

2.2 Personnel Scope

This policy applies to all personnel who operate, administer, or oversee in-scope systems, including employees, contractors, temporary staff, and third parties acting on the organization's behalf. All such personnel shall comply with this policy and its supporting standards and procedures.

2.3 Information and Systems Scope

This policy applies to all in-scope systems, devices, and services within the organization's defined boundary, whether on premises, remote, or hosted in the cloud. The systems in scope shall be identified and recorded in the asset inventory, and their compliance status shall be maintained.

2.4 Exclusions

Systems may be excluded from specific requirements only where a documented, risk-assessed exception applies, or where a system is demonstrably outside the defined scope. Exclusions shall be deliberate, recorded, and reviewed periodically to confirm they remain valid.

3. Definitions and Terminology

The following terms are used throughout this policy. Definitions are provided to ensure common understanding and consistent application.

3.1 Network and Boundary Concepts

Term	Definition
Boundary firewall	A device or service that controls traffic between the organization's network and untrusted external networks such as the internet.
Host-based firewall	Firewall functionality running on an individual device, controlling traffic to and from that device.
Network segmentation	The division of a network into zones so that traffic between zones can be controlled and a compromise contained.
Default deny	A configuration stance in which all traffic is blocked unless explicitly permitted by a rule.

3.2 Rules and Services

Term	Definition
Firewall rule	A configured statement that permits or denies specified traffic based on source, destination, port, and protocol.
Inbound service	A service reachable from an external or untrusted network, which represents exposure that must be justified and protected.
Administrative interface	An interface used to manage a device, which must not be exposed to untrusted networks without strong protection.

4. Related Documents

This policy operates within the organization's wider policy framework and is supported by the documents below. Where this policy sets a requirement, the supporting standards and processes define how it is implemented in practice.

4.1 Supporting Policies

Document ID	Document Title	Description
POL-ISMS	Information Security Policy	The top-level policy under which this policy sits.
POL-SC	Secure Configuration Standard	Secure configuration of network devices and firewalls.
POL-UAC	User Access Control Policy	Control of administrative access to network devices.
POL-CL	Cloud Security Policy	Network controls applied to cloud-hosted infrastructure.

4.2 Supporting Standards

Document ID	Document Title	Description
[STD-XXX]	Firewall Configuration Standard	Detailed firewall rule conventions and device hardening settings.

4.3 Supporting Processes

Document ID	Document Title	Description
[PRO-XXX]	Firewall Rule Change Process	How firewall rule changes are requested, approved, and recorded.

4.4 Document Availability

Supporting documents are maintained in the organization's document management system and are available to personnel according to their roles. Where a referenced document has not yet been established, the requirement in this policy still applies and the supporting document shall be developed as part of implementation.

5. Network Security Principles

The organization's approach to firewall and network security is guided by the following principles.

- Every in-scope device shall be protected by a boundary firewall or, where that is not feasible, a host-based firewall configured to equivalent effect.
- Network access shall follow a default-deny stance: traffic is permitted only where there is a documented, justified business need.
- Inbound services exposed to untrusted networks shall be minimized, justified, and protected.
- Administrative access to network devices shall be restricted and shall not be exposed to untrusted networks without strong protection.
- Firewall configuration shall be controlled through change management and reviewed regularly.

6. Boundary Protection

6.1 Boundary Firewalls

Every in-scope network shall be protected at its boundary with untrusted networks by a correctly configured firewall or equivalent network device. Where a device connects directly to an untrusted network without the protection of such a boundary, a host-based firewall shall be configured to provide equivalent protection.

Boundary firewalls shall be configured to deny traffic by default, permitting only traffic that is explicitly required and approved. The default configuration supplied by the vendor shall be reviewed and hardened before the device is brought into use.

6.2 Default Credentials and Hardening

Default administrative passwords on firewalls and network devices shall be changed to strong, unique values, or the accounts disabled, before the device enters service. Unnecessary services, features, and accounts on network devices shall be disabled in accordance with the secure configuration standard.

7. Access Control at the Network Boundary

7.1 Inbound Access

Inbound access from untrusted networks shall be permitted only to services with a documented business need, and each such service shall be justified, recorded, and protected. Services that are no longer required shall have their inbound access removed. The number of services exposed to untrusted networks shall be kept to the minimum necessary.

Where a service must be exposed, it shall be protected through measures appropriate to its risk, which may include restricting the permitted sources, requiring authentication, and ensuring the service is patched and securely configured.

7.2 Outbound and Inter-Zone Access

Outbound access and traffic between internal network zones shall be controlled where doing so limits the organization's exposure or constrains an attacker's ability to move within the network. Network segmentation shall be used to separate systems of differing sensitivity and to contain the impact of a compromise.

7.3 Administrative Interfaces

Administrative interfaces of firewalls and network devices shall not be accessible from untrusted networks unless protected by strong, additional controls such as multi-factor authentication and source restriction. Administrative access shall be restricted to authorized personnel and logged.

8. Configuration Management and Review

8.1 Rule Change Control

Changes to firewall rules and network device configuration shall be requested, justified, approved, and recorded through the change management process. Each rule shall have a recorded business justification and owner so that its continued need can be assessed.

Firewall rule sets shall be documented and maintained so that the current configuration is known and auditable.

8.2 Periodic Review

Firewall rules and network configuration shall be reviewed at defined intervals to confirm that each rule remains justified, that no unnecessary access has accumulated, and that the configuration still reflects the organization's needs. Rules that are no longer required shall be removed. Review outcomes shall be recorded.

9. Remote and Wireless Connectivity

9.1 Remote Access

Where the network is reached remotely, including by homeworkers and mobile staff, remote connections shall be authenticated and encrypted, and shall terminate at a controlled point where boundary protection applies. Remote access shall require multi-factor authentication and shall be restricted to authorized users and devices. Split-tunneling and other configurations that bypass the organization's controls shall be permitted only where justified and risk-assessed.

Remote access infrastructure shall itself be treated as an exposed, internet-facing service: kept patched, securely configured, and monitored, because it is a frequent target of attack.

9.2 Wireless Networks

Wireless networks that provide access to the organization's systems shall be secured with strong authentication and encryption and shall be segregated from networks intended for guests or untrusted devices. Guest wireless shall not provide access to internal systems. Wireless access points shall be configured to the secure configuration standard and shall not retain default credentials or insecure protocols.

10. Roles and Responsibilities

10.1 Senior Management

Senior management is accountable for ensuring that the organization establishes and maintains the controls described in this policy. Senior management shall approve this policy, ensure that adequate resources are allocated to its implementation, and accept residual risk where controls cannot fully meet the policy's objectives.

10.2 Chief Information Security Officer

The Chief Information Security Officer, or the equivalent information security function, owns this policy and is responsible for setting and maintaining its requirements and supporting standards. The function shall oversee compliance, ensure that relevant risks are reflected in the risk register, and report on the effectiveness of these controls to governance bodies.

10.3 IT Operations

IT Operations is responsible for implementing, configuring, and maintaining the technical controls described in this policy in accordance with the supporting standards and procedures. This includes day-to-day operation, monitoring, and the prompt remediation of identified weaknesses.

10.4 System and Asset Owners

System and asset owners are responsible for ensuring that the systems and information they own are protected in accordance with this policy. Owners shall confirm that their assets are within scope, participate in reviews affecting them, and accept residual risk within their delegated authority.

10.5 Third Parties and Service Providers

Third parties and managed service providers who operate in-scope systems on the organization's behalf shall meet the requirements of this policy and shall provide evidence of compliance on request. Their responsibilities shall be defined in the relevant contract or agreement.

11. Monitoring and Review

11.1 Monitoring

Firewall and network devices shall be monitored for availability, configuration change, and security-relevant events in accordance with the logging and monitoring policy. Unauthorized or unexpected configuration changes shall be alerted and investigated.

11.2 Review and Continual Improvement

This policy and the organization's firewall and network security arrangements shall be reviewed at least annually and on significant change to the network or threat environment. Reviews shall consider rule-set hygiene, exposed services, review outcomes, and incidents, and shall drive improvements.

12. Compliance and Enforcement

12.1 Compliance Expectations

Compliance with this policy is mandatory for all personnel and third parties within its scope. Compliance shall be verified through monitoring, review, and audit. Records demonstrating compliance shall be maintained and made available for review.

12.2 Exception Management

Any departure from this policy shall be managed as a documented exception that records what is excepted, the business reason, the compensating controls, the residual risk accepted, the approving authority, and a review date. Exceptions shall be time-bound, recorded in the risk register, and reviewed on expiry. An exception is not a permanent waiver.

12.3 Enforcement

Breaches of this policy shall be addressed in accordance with the organization's disciplinary process for personnel and the relevant contractual provisions for third parties. Where a breach creates a security risk, it shall be remediated as a priority and recorded as an incident where appropriate.

13. Document Control

13.1 Document Information

Attribute	Details
Document Title	Firewall and Network Security Policy
Document ID	POL-FW
Version	1.0
Classification	Internal Use
Effective Date	March 1, 2026
Next Review Date	March 1, 2027
Document Owner	Rachel Okafor, Chief Information Security Officer
Approved By	David Whitfield, Chief Executive Officer

13.2 Revision History

Version	Date	Author	Description of Changes
1.0	March 1, 2026	Information Security Team	Initial issue.

13.3 Approval

This policy has been reviewed and approved by the following authorities. Approval signifies acceptance of the policy and commitment to its enforcement.

Role	Name	Signature	Date
Chief Executive Officer	David Whitfield		
Chief Information Security Officer	Rachel Okafor		
Chief Information Officer	Phil Greaves		

Appendix A: Policy Acknowledgment Form

All personnel within scope of this policy are required to acknowledge that they have read, understood, and agree to comply with it. Completed acknowledgments are retained as a record of compliance.

I acknowledge that I have read and understood this policy and agree to comply with its requirements. I understand that failure to comply may result in disciplinary action.

Employee Name:	
Employee Signature:	
Date:	
Department:	
Manager Name:	
Manager Signature:	