REMOTE ACCESS 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 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to Employees 3

1.3.1 Applicability to External Parties 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Approved Connections 4

2.2 Remote Access Mechanism Approval 4

2.3 Perimeter Firewalls 4

2.4 Entry and Segmentation 4

2.5 Authentication and Encryption 4

2.6 Multi-Factor Authentication 4

2.7 Single Network Connections 4

2.8 Anti-Malware 4

2.9 Third Party Connections 4

2.10 Review and Removal 5

2.11 Remote Access Logging & Monitoring 5

2.12 Administration Software 5

3. Policy Compliance & Enforcement 6

3.1 Compliance Measures 6

3.2 Enforcement 6

4. Exception Process / Glossary 7

4.1 Exception Process 7

4.2 Glossary / Acronyms 7

5. Document Management 8

5.1 Document Revision Log 8

5.2 Document Ownership 8

5.3 Document Coordinator 8

5.4 Document Approvers 8

5.5 Document Distribution 8

# 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 for establishing remote access connections and ensuring only authorised users gain access to the XXXX. (XXXX) network(s) via external connections. This policy includes all forms of remote access into the XXXX organisation. This includes, but is not limited to, virtual private networks (VPN), point-to-point (P2P), dial-up, and wireless connections established by individuals employed or contracted by XXXX.

## 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.

## Related Documents / References

* *XXXX-POL-ALL-001- Information Security Policy Framework*
* *XXXX-POL-ALL-009 - Access Control Policy*
* *XXXX-POL-ALL-012- Incident Response Policy*
* *XXXX-POL-ALL-021 - Vendor Management & Due Diligence Policy*
* *XXXX-STD-ALL-009 - Logging & Monitoring Standard*
* *XXXX-PRC-ALL-025 - Policy Exception Procedure*

# Policy Statements

## Approved Connections

Remote access to the XXXX network must only be established using approved connection methods and comply with *XXXX-POL-ALL-009 - Access Control Policy*.

## Remote Access Mechanism Approval

All remote access and external connection mechanisms must be individually identified and approved by the Information Security Committee and will be recorded in an inventory (or equivalent).

Use of remote administration software, outside of the application and infrastructure support and administration teams, must be approved by Information Security Committee

## Perimeter Firewalls

All remote access must be appropriately controlled through a firewall or equivalent. Access must be limited to authorised remote access connections only.

## Entry and Segmentation

All remote access must be restricted to dedicated entry points and required appropriate network segmentation.

## Authentication and Encryption

All remote access over public networks must be authenticated and strongly encrypted.

## Multi-Factor Authentication

All remote access connections must utilise, at a minimum, Two-factor authentication (2FA) mechanisms.

## Single Network Connections

Once a staff member (includes XXXX employees, consultants and contractors) establishes a remote access connection, that user must not be connected at the same time to any other network (i.e. no split-tunnelling).

## Anti-Malware

All desktops, laptops and servers connected to XXXX networks via remote access technologies must use up-to-date anti-malware software or equivalent.

## Third Party Connections

IDs used by vendors to access, support, or maintain system components via remote access must comply with the following:

* Are enabled only during the time-period needed and disabled when not in use; and
* Are monitored when in use; and
* comply with requirements as stated in the *XXXX-POL-ALL-021 - Vendor Management & Due Diligence Policy*.

## Review and Removal

Individual remote access and remote access connections must be reviewed at least bi-annually by Information Technology and removed promptly when no longer required. Any dedicated hardware and software components of the remote access connection must also be disabled or removed.

## Remote Access Logging & Monitoring

Systems must log relevant activity. Logs must be reviewed and retained in accordance with *XXXX-STD-ALL-009 - Logging & Monitoring Standard*.

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

## Administration Software

Use of remote administration software, outside of the application and infrastructure support and administration teams, will be documented and approved by Information Security Committee

# 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 remote access connections, evidence that the methods for remote access are approved | * Signed User Access Request form/mails * Workflow tickets with approval information * Email documentation of approval * Committee or other meeting minutes (new project approvals, etc.) |
| For a selection of remote access connections, evidence that the connections are appropriately controlled through a firewall and limited to only authorized users | * System / network configuration documentation * Network diagrams * Firewall rules |
| For a selection of remote access connections, evidence that the connections enter the network through a dedicated entry point | * System / network configuration documentation * Network diagrams |
| For a selection of remote access connections, evidence that the connection only provides access to required network segments | * System / network configuration documentation * Network diagrams * Firewall / Routers rules / ACLs |
| For a selection of remote access connections, evidence that the connections are encrypted | * System configuration documentation * Example traffic packet |
| For a selection of remote access connections, evidence that the connections are authenticated prior to access | * System configuration documentation * Example authentication (screen shot) |
| For a selection of remote access connections, evidence that the connections are reviewed periodically and effective action is taken from the review | * Review and sign-off of documentation (e.g., connection list, diagrams, etc.) by appropriate personnel |
| For a selection of third-party remote access connections, evidence of the documented connection configurations or settings | * System / network configuration documentation |

## 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

|  |  |
| --- | --- |
| VPN | Virtual Private Network |
| Two-Factor Authentication | An extra layer of protection used to ensure the security of online accounts beyond just a username and password |
| 2FA | Two-Factor Authentication |
| MFA | Multi-Factor Authentication |

# 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:

* All Staff