Remote Access Policy

# Template

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

## Purpose

The purpose of this policy is to define the rules and requirements for connecting to <organisation>’s network from any host (smartphones, tablets, laptops).

These rules and requirements are designed to minimise risk that may result from unauthorised use of our resources. Risks include:

* the loss of sensitive or organisation confidential data
* the loss of intellectual property
* damage to public image
* damage to critical internal systems
* fines or other financial liabilities incurred as a result of those losses

## Applicability

This policy applies to all employees, volunteers, contractors, authorised third parties, vendors and agents with a computer or workstation used to connect to our network. This policy applies to remote access connections used to do work on our behalf, including reading or sending email and using internal resources. This policy covers all technical implementations of remote access used to connect to our networks.

## Policy

It’s the responsibility of our employees, contractors, vendors and agents with remote access privileges to our network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

General access to the internet for recreational use through our company network is strictly limited to our employees, contractors, vendors and agents, referred to as ‘Authorised Users’ (AUs). When accessing our network from a personal computer, AUs are responsible for preventing access to any computer resources or data by non-AUs.

Performance of illegal activities through our network by any user (authorised or otherwise) is prohibited. The AU bears responsibility for and consequences of any misuse of access. For further information and definitions, see our ‘Acceptable Use Policy’.

## Connection Procedures

1. Secure remote access will be strictly controlled with encryption through our Virtual Private Networks (VPNs) and strong passwords or pass-phrases. For further information see our ‘Encryption Policy’ and ‘Password Policy’.
2. AUs shall protect their login and password, even from family members.
3. While using computers to remotely connect to our corporate network, AUs shall ensure the remote host is not connected to any other network at the same time. An exception to this is protected personal networks that are under their control or the control of an AU or third party.
4. Use of external resources to conduct <organisation> business must be approved in advance.
5. All hosts that are connected to <organisation>’s internal networks through remote access technologies must use the most up-to-date anti-virus software, which includes personal computers.
6. Personal equipment used to connect to our networks must be approved, meeting the same requirements of <organisation> owned equipment for remote access.

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

## Compliance

Non-compliance with this policy may lead to disciplinary action.

Review of this document: annually by <role>.

Next review date: <date month year>.