HEALTHCARE AND BUSINESS RESOURCE

# Secure Remote Access Policy Template

A policy starting point for controlling staff, vendor and IT-provider access to important business and healthcare systems.

| | |
|---|---|
| REVIEWED | Ashley Tietze, Managing Director |
| UPDATED | 3 August 2026 |
| USE | Planning aid - not a compliance certification |

# How to use this resource

Work through each item with the people responsible for the process. Record evidence, an owner and a realistic due date for every gap. The online version provides related guidance and service links.

## 01 Required policy controls

### 1 Approved services only

Use services approved and centrally managed by the organisation or authorised IT provider.

Evidence / owner / due date: _____

### 2 Individual identity and MFA

Require individual accounts and MFA. Do not permit shared remote-access accounts.

Evidence / owner / due date: _____

### 3 Least privilege

Limit access to the approved role and use separate controlled administrator accounts.

Evidence / owner / due date: _____

### 4 Managed devices

Allow sensitive access only from devices meeting security, encryption and monitoring requirements.

Evidence / owner / due date: _____

## 02 Operational requirements

### 1 Access approval

Record the purpose, approver, systems and expiry or review date.

Evidence / owner / due date: _____

### 2 Vendor access

Enable it for an agreed period, monitor where appropriate and remove promptly.

Evidence / owner / due date: _____

### 3 Logging and review

Log authentication and administration where supported and review rights regularly.

Evidence / owner / due date: _____

### 4 Safe working

Prevent unauthorised viewing and storage on unmanaged devices; end unattended sessions.

Evidence / owner / due date: _____

## 03 Incident and exception handling

### 1 Report suspicious activity

Escalate unexpected MFA prompts, remote windows, alerts or unexplained tools.

Evidence / owner / due date: _____

### 2 Revoke before investigating

Authorised personnel may disable sessions or accounts while preserving evidence.

Evidence / owner / due date: _____

### 3 Document exceptions

Record need, risk, compensating controls, owner, approval and expiry.

Evidence / owner / due date: _____

### 4 Review the policy

Review annually and after incidents, technology changes or insurer requirements.

Evidence / owner / due date: _____

**IMPORTANT CONTEXT**

Adapt and approve this policy for your organisation. Align it with employment arrangements, contracts, privacy requirements, cyber insurance conditions and current technical controls.

**Open the current online guide and related resources**

Podium IT | (03) 8578 3077 | podiumit.com.au