Remote Access Security Policy

Purpose of this policy

The ability to securely and reliably connect to the Department of Planning, Housing and Infrastructure's (the department) Information and Communications Technology (ICT) resources from a remote location allows Flexible Working arrangements and facilitates employees' productivity.

This policy describes the department's approach to safeguarding sensitive information and information systems via approved remote access. It aims to provide a secure and consistent approach to remote access where confidentiality, integrity, authentication, and non-repudiation of information are maintained. It is aligned with the Australian Cyber Security Centre Information Security Manual.

To whom this policy applies

This policy applies to all employees who access, implement and manage information and information systems for the department remotely, with or without departmental devices (including individuals seconded from other organisations, volunteers, contingent or labour-hire workers, professional services contractors and consultants)

Policy statement

Risk-based approach

Remote access controls are implemented following a risk-based approach that considers the sensitivity of the information and information systems the controls are planned to protect. The implementation of remote access controls does not alter the sensitivity of the information and information systems. This policy limits the ability of the information and information systems to be accessed by an unauthorised user, external to the department's network.

The methods of remote access include Virtual Private Network (VPN), virtual desktop and applications and cloud based systems.

Virtual private network

Configuration of departmental VPN's should adhere to the Cyber Security Assurance Standard and Communications Security Standard. Access must also adhere to the Access Control Policy with an appropriate Multi-factor authentication mechanism implemented.

Virtual desktop and applications

Configuration of departmental virtual desktop and virtual application systems should adhere to the Cyber Security Assurance Standard and associated documents.

Cloud based systems

Cloud based systems that are accessible without a VPN or virtual desktop/application must adhere to the Cyber Security Assurance Standard, associated documents and best practice guidelines for the specific system.

Log management

Logging of systems that provide remote access should adhere to the Operations Security Standard.

Mobile device management

For portable departmental owned devices, devices must be enrolled in a departmental Mobile Device Management (MDM) system. The configuration of policies on an MDM system is to adhere to the MDM Device Standard.

Bring your own smart device

To access certain systems remotely with your own smart device requires agreement to enrol your device in the department MDM system. The policies applied to your personal device are documented in the BYOSD App Protection Policies document and requires the end user to agree to the Bring Your Own Smart Device (BYOSD) Usage Agreement.

Exemptions

- Exemptions to this policy must comply with the ISMS Exemption Request Management Standard.
- Exemptions must only be approved where it is technically, practically or financially infeasible to comply with this policy.
- Reviews of exemptions must be performed annually.

Failure to comply with this policy

Ethical and behavioural standards that employees are expected to demonstrate while working with the department are set out in the Code of Ethics and Conduct. If employees fail to meet those standards, corrective action may be taken in accordance the Code of Ethics and Conduct.

Individuals who are not government sector employees such as volunteers, contingent or labour hire workers, professional services contractors and consultants may have their services, contract or agreement terminated immediately, or legal action could be taken if they are found to have violated this policy.

Review timeframe

Digital Information Office will review this policy no later than 3 years from the date the document is approved. This policy may be reviewed earlier in response to post-implementation feedback, changes to legislation, or as necessary in accordance with the department's policy and procedures.

Related documents

This policy should be read in conjunction with the following documents:

- Cyber Security Policy
- Access Control Policy
- Acceptable Use Policy
- ISMS Exemption Request Management Standard
- Code of Ethics and Conduct
- Mobile Device Policy - Corporate and BYOD
- Cyber Security Assurance Standard
- Operations Security Standard
- Communications Security Standard

Policy metadata

Table 1. Policy metadata

Category	Description
Status	Final
Date of approval	27.05.2021
Approver	Deputy Secretary
Group	Corporate Services
Division	Digital Information Office
Policy owner	Chief Digital and Information Officer
Document location	DPHI intranet
Next review date	April 2026
Associated procedure	N/A
Any additional applicability	Additional applicability will be considered in the future
Superseded document	N/A
Further information	cybersecurity@dpie.nsw.gov.au
Document Reference	POL21/15

Version control

Table 2. Version Control

Version	Date issued	Change
1	27.05.2021	New Policy
1.1	03.05.2022	Updated to reflect new branding and name change.

Version	Date issued	Change
1.2	12.02.2024	Updated to reflect new branding and name change. Removed internal links.

Appendices

Appendix 1 – Definitions

Appendix 2 - Roles and responsibilities

Appendix 1 – Definitions

Table 3 - Definitions

Term	Definition
Access control	To ensure that access to assets is authorized and restricted based on business and security requirements.
Cloud	Servers that are accessed over the internet, and the software and databases that run on those servers.
Mobile device	A portable computing or communications device.
Multi-factor authentication	An authentication method that requires a user to provide two or more factors to authenticate. Usually requires something you know (password) and something you have (soft token, hard token, one time password), in order to confirm the legitimacy of your identity for an online transaction or to gain access to an application.
Remote access	Access to a system that originates from outside an organisation's network and enters the network through a gateway, including over the internet.
Virtual application	Provides a virtualisation solution for application delivery to any device over any network.
Virtual desktop	Provides a virtualisation solution for desktop delivery to any device over any network.

Appendix 2 - Roles and responsibilities

Table 4: Roles and responsibilities

Role	Responsibility
Chief Digital and Information Officer (CDIO)	• Approve exemptions to this policy.
Digital and Information Office (DIO)	• Must implement this policy. • Notify Chief Information Security Officer (or equivalent) of any changes.
Chief Information Security Officer (or equivalent)	• Must develop, maintain and improve this policy. • Monitor and report on compliance to this policy (effectiveness measurements). • Review exemptions to this policy.
Employees	• Must apply to Digital Information Office to get a remote access VPN token (hardware or software). • If not connecting via corporate VPN, must ensure that departmental device is brought back to the office and connected directly to the network, at least every month, to ensure any out-of-date patches, cached process, etc. are updated. Failure to comply could result in the asset being removed from the network. • When working remotely, employees must utilise, whenever possible, their own private internet connection (ADSL, NBN, Mobile Data) to avoid sensitive information being intercepted whilst being transmitted over the internet. Public Wi-Fi should not be utilised for business purposes.