

Internet & Network Use Policy

For Australian Small & Medium Enterprises

Template Version 1.0 | December 2024

Important Notice

This template provides general guidance on internet and network use. Tailor the policy to reflect your organisation's specific requirements and ensure compliance with workplace monitoring and privacy laws.

1. Purpose

This policy establishes guidelines for the appropriate use of internet access and network resources at [Company Name]. It aims to ensure productive use of technology resources while protecting the organisation from security threats and legal risks.

2. Scope

This policy applies to:

- All employees, contractors and authorised users
- All internet access provided by [Company Name]
- All network resources and infrastructure
- All devices connected to the company network

3. General Principles

Internet and network resources are provided primarily for business purposes. Users should:

- Use resources responsibly and professionally
- Protect network security
- Respect bandwidth and shared resources
- Comply with all laws and company policies

4. Acceptable Use

4.1 Business Use

Internet and network access should be used for:

- Work-related research and information gathering
- Business communications
- Accessing work applications and systems
- Professional development and training

- Industry news and updates

4.2 Personal Use

[Company Name] permits limited personal use provided it:

- Does not interfere with work duties
- Is kept to a minimum during work hours
- Does not consume excessive bandwidth
- Complies with all other policy requirements
- Is conducted during breaks where possible

5. Prohibited Activities

The following activities are strictly prohibited:

5.1 Illegal Activities

- Accessing, downloading or distributing illegal content
- Copyright infringement and piracy
- Hacking, cracking or unauthorised access attempts
- Gambling where illegal
- Any activity that violates Australian law

5.2 Inappropriate Content

- Accessing sexually explicit material
- Accessing violent, hateful or discriminatory content
- Accessing content that would constitute harassment
- Offensive material that violates workplace standards

5.3 Security Risks

- Downloading unauthorised software
- Bypassing security controls or filters
- Connecting unauthorised devices to the network
- Disabling security software
- Sharing network credentials

5.4 Resource Misuse

- Excessive streaming of non-work content
- Running personal businesses
- Large file downloads unrelated to work
- Activities that degrade network performance

6. Social Media and Online Services

When accessing social media and online services:

- Do not share confidential business information
- Do not make statements that could harm the company
- Be mindful that personal posts may reflect on the employer
- Follow the company's social media policy
- Do not use company systems for personal social media excessively

7. Downloads and Software

7.1 Software Installation

- Only install software approved by IT
- Request software through proper channels
- Do not install unlicensed software
- Do not install software that may pose security risks

7.2 File Downloads

- Only download files required for work
- Scan downloads for viruses before opening
- Be cautious of files from unknown sources
- Report suspicious downloads to IT

8. Network Security

8.1 User Responsibilities

- Do not share network passwords
- Do not attempt to access systems without authorisation
- Report suspicious network activity
- Follow secure practices when using wireless networks
- Lock workstation when away from desk

8.2 Wireless Network Use

- Use only approved wireless networks
- Be cautious on public Wi-Fi
- Use VPN when accessing company resources remotely
- Do not set up personal wireless access points

9. Remote Access

When accessing company networks remotely:

- Use approved VPN connections
- Ensure the remote device meets security requirements
- Do not use untrusted networks for sensitive work
- Follow the same policies as when in the office
- Secure the physical environment

10. Bandwidth Management

[Company Name] may implement measures to manage bandwidth:

- Prioritisation of business-critical applications
- Throttling of non-essential traffic during peak times
- Blocking of bandwidth-intensive sites
- Usage monitoring and reporting

11. Monitoring

[Company Name] monitors internet and network use:

- For security purposes
- To ensure policy compliance
- To manage network resources
- As permitted by law

Users should have no expectation of privacy when using company internet and network resources. Monitoring may include websites visited, files downloaded, and bandwidth usage.

12. Content Filtering

[Company Name] may implement content filtering to:

- Block access to prohibited categories of websites
- Prevent malware and security threats
- Enforce policy compliance
- Protect network resources

If legitimate business access is blocked, request access through IT.

13. Reporting Incidents

Report the following to IT immediately:

- Suspected malware or virus infections

- Accidental access to inappropriate content
- Security vulnerabilities discovered
- Suspicious network activity
- Policy violations by others

14. Responsibilities

14.1 Users

- Use internet and network resources responsibly
- Protect security and report threats
- Comply with this policy

14.2 IT Department

- Maintain network security
- Implement appropriate controls
- Respond to security incidents
- Provide approved access to resources

14.3 Management

- Ensure team awareness of policy
- Address policy breaches
- Model appropriate behaviour

15. Policy Breaches

Breaches of this policy may result in:

- Restriction of internet access
- Disciplinary action
- Termination of employment for serious breaches
- Legal action where appropriate

16. Review

This policy will be reviewed:

- At least annually
- When technology or threats change
- When business needs change

Employee Acknowledgement

I acknowledge that I have read and understood [Company Name]'s Internet & Network Use Policy. I understand the expectations for appropriate use and agree to comply with this policy.

Employee Name: _____

Signature: _____

Date: _____