FREE TEMPLATE — CANADIAN EDITION

Remote Work Security Policy Template

Covering Device Management, VPN, BYOD, Data Handling & Acceptable Use

DSIT Professional Services Inc. | dsitpro.com | Ontario, Canada

Purpose	Provide a ready-to-customize remote work security policy for Canadian businesses
Applies To	All employees, contractors, and agents who access company systems from outside the primary office
Instructions	Replace all [BRACKETED] fields. Have legal counsel review before finalizing. Obtain signed acknowledgement from all staff.
PIPEDA Note	This policy supports your PIPEDA Principle 7 (Safeguards) obligations for remote access scenarios.

POLICY HEADER

Policy Title	Remote Work and Mobile Device Security Policy
Effective Date	[Date]
Approved By	[Name, Title]
Review Date	[Date — annually recommended]
Applies To	All employees, contractors, and third parties accessing [Organization Name] systems remotely

1. PURPOSE

This policy establishes security requirements for all personnel who access [Organization Name] systems, data, or applications from outside the primary workplace, including from home, client sites, or public locations.

The goal is to protect [Organization Name] data and client information from unauthorized access, disclosure, and loss while enabling productive remote work.

2. APPROVED DEVICES

Only [Organization Name]-issued devices, or personally-owned devices approved and enrolled in [Organization Name]'s Mobile Device Management (MDM) system, may be used to access company systems.

Approved devices must: have full disk encryption enabled, have current operating system and security updates applied, have approved antivirus/EDR software installed, be enrolled in MDM with [Organization Name] as the managing entity.

Unapproved devices — including family members' computers, shared devices, or devices that cannot be enrolled in MDM — must not be used to access company systems under any circumstances.

3. REMOTE ACCESS REQUIREMENTS

All remote access to [Organization Name] systems must be made via the approved VPN: [VPN Product Name].

VPN must be connected before accessing any company systems, files, or email from outside the office.

Split tunneling is not permitted — all traffic must route through the corporate VPN when connected.

VPN credentials must not be shared with any other person, including family members or colleagues.

VPN access is automatically terminated after [X hours] of inactivity.

4. MULTI-FACTOR AUTHENTICATION (MFA)

MFA is mandatory for all remote access to [Organization Name] systems including email, file storage, and business applications.

Approved MFA methods: [list approved methods e.g. Microsoft Authenticator, hardware key].

SMS-based MFA is not permitted for highly sensitive systems — use an authenticator app.

MFA recovery codes must be stored securely and not shared.

5. PASSWORD REQUIREMENTS

All passwords must be a minimum of 14 characters and include uppercase, lowercase, numbers, and symbols.

Passwords must not be reused across accounts.

A corporate password manager ([Product Name]) is provided to all staff — use is mandatory for all work accounts.

Passwords must not be written down, stored in plain text, or shared with colleagues.

6. PUBLIC WI-FI AND WORKING IN PUBLIC

Public Wi-Fi networks (coffee shops, airports, hotels) must never be used to access company systems without the approved VPN connected.

Staff must ensure screens are not visible to others when working with sensitive information in public.

Devices must be physically secured when unattended — never leave a device unlocked and unattended in a public place.

7. DATA HANDLING

Company and client data must not be stored on personal cloud services (personal Google Drive, iCloud, Dropbox) — use only approved company storage: [approved storage platform].

Sensitive documents must not be printed at home unless specifically authorized and the printed copy is destroyed immediately after use.

Confidential data must not be discussed in public locations where it can be overheard.

USB drives and external storage are prohibited unless specifically authorized and encrypted.

8. INCIDENT REPORTING

Any lost or stolen device must be reported to [Privacy Officer / IT contact] immediately — within 1 hour of discovery.

Any suspected security incident, including suspicious emails, unauthorized access attempts, or malware alerts, must be reported immediately.

Remote device wipe will be performed on any lost or stolen device enrolled in MDM.

9. POLICY VIOLATIONS

Violations of this policy may result in disciplinary action up to and including termination.

Policy violations involving client data may trigger regulatory reporting obligations under PIPEDA or sector-specific laws.

Staff who discover a potential policy violation by a colleague must report it to [reporting contact].

10. ACKNOWLEDGEMENT

All staff must sign the Remote Work Policy Acknowledgement Form confirming they have read, understood, and agree to comply with this policy.

Signed acknowledgements must be retained in personnel files.

This policy must be re-acknowledged annually and when significant updates are made.

STAFF ACKNOWLEDGEMENT FORM

Detach and retain signed copies in personnel files.

Employee / Contractor Name	_____
Role / Department	_____
Signature	_____
Date	_____

Manager Name	_____

I confirm that I have read, understood, and agree to comply with the [Organization Name] Remote Work and Mobile Device Security Policy. I understand that violations may result in disciplinary action.