TELEWORKING SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.0
Published: September 2019
Table of Contents

I  INTRODUCTION, SCOPE, BACKGROUND .................................................................................. 3
II  GLOSSARY, TERMS AND DEFINITIONS, LIST OF COMMONLY USED REFERENCES ............... 3
1  TELEWORKING .......................................................................................................................... 4
1.1  TELEWORKING ....................................................................................................................... 4
I  Introduction, Scope, Background

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: IM/IT Standards).

II  Glossary, Terms and definitions, List of commonly used references

To avoid repetition of content, please check the “Glossary”, “Terms and definitions” and “List of commonly used references” sections of the Information Security Standard (version 2.0) (published here: IM/IT Standards) for the terms and definitions used in this standard.
1 Teleworking

1.1 Teleworking

1.1 Teleworking must employ security controls to ensure that information resources are not compromised.
   a) Teleworking security controls
   b) Teleworking agreement
   c) Ad hoc teleworking policy

**Purpose:** To protect information accessed through teleworking arrangements from loss or unauthorized access.

1.1 a) Teleworking security controls based on risk assessment

Information Owners and Information Custodians must ensure that government information and information technology assets are adequately protected regardless of the type of access or physical location of employees. Teleworking security controls must consider:

- The sensitivity and classification of information assets that may be accessed or stored at the teleworking location (e.g., paper files, mobile devices such as laptops, smartphones, USB drives);
- The physical security of information, information technology assets and the teleworking location;
- Unauthorized information access by people at the teleworking location, either inadvertent or deliberate;
- Enrollment in Mobile Device Management Service;
- Remote access threats if remote access is utilized;
- Restriction of permitted information types and classifications at the teleworking location;
- Provision of government-managed equipment, if appropriate, due to information sensitivity or volume;
- Use of secure cabinets, shredders and other physical security equipment;
- Security awareness training for protection of information and information assets, including clear desk policy, information handling rules, physical security issues and remote access training; and,
- Monitoring and review of teleworking equipment for security events and incident response.

Sensitive and confidential information must be stored only on protected government systems, as defined in the Appropriate Use Policy.

1.1 b) Teleworking agreement

Teleworking arrangements must be formally authorized and documented.

A documented teleworking agreement between the employer and employee must exist that specifies the following employee responsibilities, terms and conditions:

- The expectation that the employee will actively protect information and information technology assets;
• Reference to the BC Public Service Agency Human Resource Policies, Oath of Employment, Standards of Conduct, Appropriate Use Policy, Information and Communications Technology (ICT) Agreement, or contract terms as appropriate;
• Restrictions on information asset types or classifications permitted at the teleworking location;
• The requirement to protect information from inadvertent or deliberate disclosure to people at the teleworking location by use of secure cabinets, passwords or shredders;
• The authorized teleworking location and contact information;
• Information availability requirements;
• What equipment and software is supplied by the employee and by the employer;
• Completion of a Home Technology Assessment;
• The terms of use for remote access, if applicable;
• The requirement to meet or exceed specified wireless networking security controls, if wireless networking will be used at the teleworking location;
• The requirement to report security events or unusual activity;
• Arrangements for technical support; and,
• The start date, end date, expected work hours and provision for termination of the teleworking arrangement.

1.1 c) Ad hoc teleworking policy
Ministries must develop and communicate policies and processes specific to their areas that govern ad hoc teleworking, in particular the practice of removing material from the workplace. Controls required for an ad hoc teleworking policy are:
• Restriction of the information asset types and classifications that may be accessed or utilized while teleworking;
• Use of secure cabinets, shredders and other physical security equipment; and,
• Minimum technical security controls required for non-government computing equipment, in particular current anti-virus, personal firewall and current software patches.

Guidelines:
Teleworking employees should use the following security measures when accessing government information services:
• Desktop Terminal Service (DTS) – preferred access method for non-government devices;
• DTS or Virtual Private Network (VPN) for government devices; and
• Application specific methods such as Secure Sockets Layer (SSL) enabled websites (e.g., Outlook Web Access).
Use of VPN access on non-government devices should be avoided, unless it is used with Remote Desktop Protocol (RDP) connection.

Recommended Tests:
Note: 1.1 is reported on as part of the annual information security review.
• Demonstrate teleworking policies and teleworking agreements are documented.
• Demonstrate Home Technology Assessments are completed.