Policy Summary No. 4
Remote Access

Information Security Branch, Office of the Chief Information Officer
Ministry of Citizens' Services, Province of British Columbia
http://www.cio.gov.bc.ca/cio/informationsecurity/index.page

Importance of Information Security

Protection of information assets is the primary goal of information security. This includes practicing safe computing behaviours to reduce the overall occurrence of theft, loss, or misuse of government information assets.

A breach in information security or loss of information assets can have serious consequences, depending on the sensitivity and value of the information and the extent of the breach. The consequences can include:

- disclosure of personal information,
- interruption in government's ability to deliver services,
- financial losses related to correcting the situation,
- threats to public safety or individuals' health and well-being,
- legal actions, and
- erosion of the public trust in the government.

Personnel action is the KEY to protecting government information assets. Technology and policies are only effective if personnel are aware of their responsibilities to use the processes enforcing the policies. Education and awareness are essential to promote an understanding of the importance of information security.

The purpose of this document is to provide guidance about security-related aspects of a subject area of interest to the government community. It outlines the subject area background, related security concerns, responsibilities, and relevant information security policy.

Subject Area Description

Remote access to government information has increased due to mobile computing and accessing information from places other than a government office. Remote access is access provided to government information and information systems from non-government locations. Remote access allows personnel to access government information from virtually any location and at any time. Remote access services are used by travelling or mobile personnel, telework or home office users and operational support personnel from permanent remote sites (PS#5 Mobile Computing, PS#14 Working from Home, PS#26 Access Control Management).

Remote access uses various technologies and techniques. Government authorized technologies include Desktop Terminal Services (DTS), Virtual Private Networking (VPN), and Outlook Web Access. These technologies are configured to provide protection of the government network, applications and information (PS#21 Operational Security, PS#20 Application Security, PS#16 Protection of Sensitive Information).

This Policy Summary offers guidance on the use of remote access services. It is intended to guide personnel and help them understand their responsibilities and obligations according to the Information Security Policy.

Areas of Concern

Unauthorized remote access to government information may lack the security controls implemented on government systems that include monitoring and logging, patching and remote access configuration management. The primary area of concern is unauthorized remote access to government information.

Many factors amplify this concern:

- Unsecured or poorly secured remote access increases security and privacy risks to information and information resources.
- Risk of theft of user credentials where remote access is unsecured and personnel are working from a location outside of their government office.
- Unauthorized disclosure, alteration, loss, or destruction of sensitive information where remote access technologies are not secured.
- Internet security controls may be improperly configured where remote access is implemented using the Internet.
- Unauthorized remote access can increase risks to information and information resources (e.g., changing firewall configuration).
- Personnel may have insufficient awareness of information protection for remote access.

Intended Outcomes

The policies associated with remote access are intended to:

- Reduce the risk of government information and network compromise.
- Reduce the occurrence of unauthorized access and use of government information and networks.
- Increase awareness of the consequences caused by unsecured remote access.

Responsibilities of all Personnel

Things to do:

- Actively protect government information and information systems when using remote access services.
- Be aware of and understand security policy and practices for sensitive information.
- Only use secure access protocols and services when accessing government applications and servers, e.g., Virtual Private Network (VPN), Desktop Terminal Service (DTS), and Outlook Web Access.
- Do not use public computers to access sensitive information when using the Internet.
- Attend information security awareness, education and training offerings.

Things to avoid:

- Unauthorized access to government equipment or remote access accounts.
- Bypassing or disabling the security protections and controls set on government issued mobile devices.
- Downloading or using unauthorized software on government computers.

Things to pay attention to:

- When using remote access, be aware of potential threats associated with the location and environment.
- Be aware of what and who is in the environment you are working remotely from.

Things to report:

- Actual and suspected security incidents and events as required by the Information Incident Management Process.
- File a General Incident or Loss Report (GILR) within 24 hours of a security incident.

Responsibilities of Management

Things to do:

- Authorize employees to access government information systems only when there is a business requirement.
- Consider risks prior to granting contractors remote access privileges.
- Ensure remote users connect through authorized remote access services or secure gateway services, e.g., Virtual Private Network (VPN), Desktop Terminal Service (DTS), and Outlook Web Access.
- Identify, document, and maintain remote access accounts and asset inventories.
- When a security or privacy breach has occurred, review and revise related policies and processes as needed.

Things to pay attention to:

- Be aware of current standards for protecting data stored on mobile devices.
- Situations where there is access to personal and sensitive information at remote locations.

Things to establish procedures for:

- Approval process for remote access accounts.
- Documenting approved off-site remote access equipment.

Things to reinforce with personnel:

- Treat information as a valuable resource and take actions to prevent loss, destruction or inappropriate disclosure.
- Ensure the use of the Information Incident Management Process when required.

Resources

- General Incident or Loss Report (GILR) http://gilr.gov.bc.ca/
- Information Incident Reporting - Shared Services BC Service Desk at 250 387-7000 or 1-866 660-0811, Select Option 3

References

Document	Description
Core Policy and Procedures Manual http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm	
12	Information Management and Information Technology Management
12.3.1	Appropriate Use
15	Security
Information Security Policy http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf	
2.1.4	Use of non-government hardware
2.2.1	Third party remote access risk assessment
3.1.1	Asset Management – Asset Responsibility
3.1.3	Acceptable use of government resources
4.2.2	Information security awareness, education and training
5.2.5	Protection of equipment when off-site from government premises
6.4.1	Prevention and detection of malicious code
7.4.1	Network access control – Authorized access
7.4.2	Remote access to Government networks and services
Standards and Guidelines	
	IM/IT Standards Manual http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/standards_manual.pdf
	Working Outside the Workplace http://www.cio.gov.bc.ca/cio/working_outside_workplace/index.page
	Information Incident Management Process http://www.cio.gov.bc.ca/local/cio/information_incident/information_incident_management_process.pdf

Key Contacts

Contact	Link
Office of the Chief Information Officer	http://www.cio.gov.bc.ca
Information Security Branch, Office of the Chief Information Officer	http://www.cio.gov.bc.ca/cio/informationsecurity/index.page