BRITISH COLUMBIA | Ministry of Citizens' Services

COMMUNICATIONS 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

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 Communications Security

This chapter identifies the information security requirements for network and communication services.

1.1 Network security management

1.1.1	**Controls must be implemented to achieve and maintain security within the government network.** **a) Control and management of networks** **b) Configuration control** **c) Secured path** **d) Wireless Local Area Networking** **e) Equipment management** **f) Logging, monitoring and detection** **g) Coordination and consistency of control implementation**

Purpose: ***To ensure that network security controls and network security management practices are implemented and documented to maintain network security.***

1.1.1 a) Control and management of networks

Information Custodians must implement network infrastructure security controls and security management systems for networks to ensure the protection of information and attached information systems. Selection of controls must be based on a Security Threat and Risk Assessment, taking into account the information security classification determined by the Information Owners, and applicability to the network technology.

The Security Threat and Risk Assessment must consider network-related assets which require protection including:

- Information in transit;
- Stored information (e.g., cached content, temporary files);
- Network infrastructure;
- Network configuration information, including device configuration, access control definitions, routing information, passwords and cryptographic keys;
- Network management information;
- Network pathways and routes;
- Network resources such as bandwidth;
- Network security boundaries and perimeters; and,
- Information system interfaces to networks.

1.1.1 b) Configuration control

To maintain the integrity of networks, Information Custodians must manage and control changes to network device configuration information such as configuration data, access control definitions, routing information and passwords.

Network device configuration data must be protected from unauthorized access, modification, misuse or loss by the use of controls such as:

- Encryption;

- Access controls and multi-factor authentication;
- Monitoring of access;
- Configuration change logs;
- Configuration baselines protected by cryptographic checksums; and,
- Regular backups.

Status accounting must be regularly performed to ensure that configuration baselines reflect actual device configuration.

1.1.1 c) Secured path

Where required by information classification and a Security Threat and Risk Assessment, information must only be transmitted using a secured path.
Secured paths for information transmission must use controls such as:

- Data, message or session encryption, such as SSH, SSL or VPN tunnels; and,
- Systems to detect tampering.

1.1.1 d) Wireless Local Area Networking

Wireless Local Area Network access points must be authorized by the Office of the Government Chief Information Officer for attachment to the government network. Wireless Local Area Networks must utilize the controls specified by the Chief Information Security Officer and must include:

- Strong link layer encryption, such as Wi-Fi Protected Access;
- User and device network access controlled by government authentication services;
- The use of strong, frequently changed, automatically expiring encryption keys and passwords;
- Segregation of wireless networks from wired networks by the use of filters, firewalls or proxies; and,
- Port-based access control, for example use of 802.1x technology.

Where supported by the information classification or a Security Threat and Risk Assessment, additional controls for wireless networks may include:

- Virtual Private Network (VPN) tunnel technology;
- The use of Desktop Terminal Services (DTS) technology; and,
- Intrusion detection systems, firewalls and Media Access Control (MAC) address filtering.

1.1.1 e) Equipment management

Information Custodians must document responsibilities and procedures for operational management of network infrastructure, including devices at network boundaries and in user areas.

1.1.1 f) Logging, monitoring and detection

To facilitate monitoring, response and investigation, logging to a centralized log management service must be enabled, including logging of:

- Traffic traversing network security boundaries;
- Traffic within networks housing sensitive or critical systems or information;
- Security-relevant events on network devices, such as operator logon and configuration changes; and,
- Security-relevant events on systems that provide authentication and authorization services to network infrastructure devices such as routers, firewalls or switches.

Logs must be continuously monitored to enable detection and response to security events and intrusions (e.g., automation of log monitoring and event alerting). Logs from available sources (including, but not limited to, network traffic, network firewalls, Intrusion Prevention Systems, routers, switches, content filtering, servers, applications, databases, application firewalls, authentication services) must be continuously correlated to enable detection and response to security events and intrusions, that otherwise would go undetected without such correlation and alerting.

In order to support the monitoring and correlation of logs from available sources, in cases when infrastructure or services are provided via a third-party, it must be ensured that security event logs from the respective outsourced infrastructure or services can be forwarded real-time to the government centralized monitoring services to allow for the centralized monitoring, correlation and alerting across government.

Information Custodians must ensure there is a clear segregation of duties for employees involved in logging, monitoring or detection activities. Active automated surveillance of networks must be implemented to detect and report on security events (e.g., network intrusion detection systems). Sensors enabling on-demand capture of network traffic must be implemented at network security boundaries and within networks housing sensitive information or information systems as determined by a Security Threat and Risk Assessment.

1.1.1 g) Coordination and consistency of control implementation

Information Owners and Information Custodians must document network security controls in the System Security Plan including:

- A summary of risks identified in the Security Threat and Risk Assessment;
- Roles and responsibilities for network security management;
- Specific procedures and standards used to mitigate risks and protect the network;
- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures (including monitoring frequency, review and remediation processes).

Recommended Tests:

Note: 1.1.1 is reported on as part of the annual information security review.

- Demonstrate that access to the network devices is restricted and is done via central authentication and automated updates.
- Demonstrate configuration controls are established to safeguard the confidentiality and integrity of data passing across networks.
- Demonstrate controls for wireless local area networks meet the standard requirements.
- Demonstrate that network activities are monitored and logged.

1.1.2 Security configuration, service levels and management requirements of all network services must be documented and included in any network service agreement.
a) Network service agreement

Purpose: To specify what security features are required for delivery of a network service.

1.1.2 a) Network service agreement

Formal network service agreements must be established between network service providers and consumers of network services to specify service levels, services offered, security requirements and security features of network services. The network service agreement must include specification of:

- The rules of use to be followed by consumers to maintain the security of network services;
- The schedule for ongoing verification of network security controls;
- The rights of either party to monitor, audit or investigate as needed;
- Security incident response responsibilities, contacts and procedures; and,
- The requirement to meet or exceed government IM/IT Security Standards.

Information Owners and Information Custodians must confirm that the specified security features are implemented prior to commencement of service delivery.

Recommended Tests:

Note: 1.1.2 is reported on as part of the annual information security review.

- Demonstrate configuration controls are established to safeguard the confidentiality and integrity of data passing across government networks.
- Demonstrate the requirement for Security Threat and Risk Assessment is included in service level agreements for all networks.
- Demonstrate all network service arrangements have a documented network service agreement in place that specifies security features.
- Demonstrate network service provider's security controls are regularly monitored and have annual audits completed.

1.1.3 Groups of information services, users and information systems must be segregated on networks.
a) Segregation based on risk and requirements

Purpose: ***To isolate information systems, users and networks based on risk and business connectivity requirements.***

1.1.3 a) Segregation based on risk and requirements

Information Custodians must segregate services, information systems and users to support business requirements for information system connectivity and access control based on the principles of least privilege, management of risk and segregation of duties.

Information Custodians must establish network perimeters and control traffic flow between networks. Network traffic flow control points such as firewalls, routers, switches, security gateways, VPN gateways or proxy servers must be implemented at multiple points throughout the network to provide the required level of control.

The techniques and technologies selected for network segregation must be based on Security Threat and Risk Assessment and Privacy Impact Assessment findings. Factors to consider include:

- The information and information system security classification;
- The trustworthiness of the network, based on the amount of uncontrolled malicious traffic present, the level of device identification and authentication in the networks, and sensitivity to eavesdropping (e.g., the Internet is a less trusted network than a controlled server network zone);

- Transparency, usability and management costs of network segregation technologies; and,
- The availability of compensating controls for detection, prevention and correction of malicious network traffic and unauthorized access attempts.

Network zones must be defined and network perimeters established, according to business requirements and risk as identified in the Security Threat and Risk Assessment and Privacy Impact Assessment (e.g., network zones for public access, Ministry, core network, wireless network). Information system operational management and business applications must be defined and separated by network flow control points.

Guidelines:
Security gateways should be used to verify the trustworthiness of devices attempting to connect to the network (e.g., VPN Quarantine systems, network switch isolation and admission control systems).

Recommended Tests:
Note: 1.1.3 is reported on as part of the annual information security review.

- Demonstrate that access to the network by devices is restricted and is done via central authentication and automated updates.
- Demonstrate configuration controls are established to safeguard the confidentiality and integrity of data passing across public networks.
- Demonstrate configuration controls for wireless local area networks.
- Demonstrate appropriate security monitoring and logging of network activities.

1.1.4	**Networks must have routing controls to ensure that computer connections and information flows do not breach the access control policy of the information system.** **a) Network address control** **b) Control of routing information**

Purpose: ***To control network routing to prevent unauthorized access or bypassing of security control points.***

1.1.4 a) Network address control
Information Custodians must implement mechanisms to prevent network address spoofing and routing of spoofed network traffic (e.g., through use of router access control lists).
Security gateways must be considered for network access control points, in accordance with information system security classification requirements. Gateways may be used to validate source and destination addresses when proxy servers or network address translation are used with secondary identity verification techniques (e.g., user identifier and password, digital certificates).

1.1.4 b) Control of routing information
Information Custodians must implement processes and controls to prevent unauthorized access to, or tampering of, network routing information (e.g., through use of encryption, authenticated routing protocols, access control lists).

Recommended Tests:
Note: 1.1.4 is not reported on as part of the annual information security review.

- Demonstrate Information Security Threat and Risk Assessments are completed on all devices that provide network routing.

1.2 Information transfer

1.2.1	**Information exchange policies, procedures and controls must be documented and implemented to protect the exchange of information through all types of electronic communication services.** **a) Electronic information exchange**

Purpose: ***To protect information from unauthorized disclosure.***

1.2.1 a) Electronic information exchange

The Chief Information Security Officer must document and implement procedures to protect information from interception, copying, misrouting and disposal when being transmitted electronically. Transmission methods include but are not limited to:

- E-mail, including attachments;
- Electronic file transfer (e.g., File Transfer Protocol (FTP), Electronic Data Interchange (EDI));
- Use of mobile devices;
- Telephone, cell, and other voice messaging;
- Faxes; and,
- Instant messaging.

Recommended Tests:

Note: 1.2.1 is reported on as part of the annual information security review.

- Demonstrate the procedures designed to protect transferred information from interception, copying, modification, misrouting and disposal are in place.
- Demonstrate controls for detection and protection against malware are in place.
- Demonstrate employees are provided with training on recognizing phishing attempts.
- Demonstrate employees are provided with training for information exchange policies, procedures and controls.
- Demonstrate employees are provided with training on procedures for protecting information from unauthorized disclosure.

1.2.2	**Information and software exchange agreements between the Province and other organizations must address the secure transfer of information between parties.** **a) Exchange agreements** **b) Information and software exchange requirements**

Purpose: ***To protect information or software from loss or unauthorized disclosure.***

1.2.2 a) Exchange agreements

Information Owners and Information Custodians must ensure the terms and conditions for secure exchange of information assets with external parties is documented in an agreement. The agreement must define:

- Custody and control accountabilities;

- Authority of a custodian to publish, grant access to or redistribute the information;
- Purpose and authorized uses of the information or software;
- Limitations on data linkage;
- Duration, renewal and termination provisions;
- Primary contacts for agreement, governance and management;
- Requirements for:
    - Protecting information according to its security classification,
    - Handling information (e.g., recording authorised recipients, confirming receipt of transmitted data, periodically reviewing records of authorised recipients),
    - Labelling information (e.g., methods to be used to apply and recognize labelling),
    - Maintaining integrity and non-repudiation of information, and,
    - Media management and disposal;
- Technical standards for transmission, recording or reading information or software;
- Responsibilities for reporting privacy and security incidents and breaches;
- Liability, accountability and mitigation strategies, for attempted, suspected or actual privacy and security incidents and breaches; and,
- Problem resolution and escalation processes.

1.2.2 b) Information and software exchange requirements
Information Owners and Information Custodians must ensure an approved Privacy Impact Assessment and a Security Threat and Risk Assessment are completed for the information or software covered by the exchange agreement.

Exchange agreements must be reviewed by legal counsel for the Province prior to being signed.

Guidelines:
Province of B.C. Legal Services should be consulted during the development of sharing agreements.

Recommended Tests:
Note: 1.2.2 is reported on as part of the annual information security review.

- Demonstrate that exchange of information with external parties is covered by an information sharing agreement.
- Demonstrate Security Threat and Risk Assessments are completed on all information sharing agreements assessing the transfers of information.
- Demonstrate Privacy Impact Assessments are completed on all information sharing agreements.
- Demonstrate that information and software exchange agreements with external parties have been reviewed by Legal Services.

1.2.3 Information transmitted by electronic messaging must be appropriately protected.
a) General requirements
b) Custody of electronic messages

Purpose: To enable secure and trustworthy electronic messaging

1.2.3 a) General requirements
Electronic messaging services must be managed to protect the integrity of government messages by:

- Protecting messages from unauthorized access, modification or denial of service;

- Ensuring correct addressing and transportation of messages;
- Providing reliable and available messaging infrastructure; and,
- Conforming to legislative, regulatory, standards and policy requirements.

The Government Chief Information Officer must approve implementation of, and significant modification to, electronic messaging systems.

Employees must support the responsible use of electronic messaging services by:

- Using only government electronic messaging systems for conducting government business, including systems for remote access to government messaging systems from publicly available networks;
- Using only authorized encryption for e-mail or attachments;
- Not automatically forwarding government e-mail to external e-mail addresses; and,
- Maintaining the confidentiality and privacy of information being communicated in electronic messages as appropriate to the sensitivity and classification of the information.

Information Owners must authorize and approve the use of social media services and other non-government electronic messaging services for conducting government business.

1.2.3 b) Custody of electronic messages

Electronic messages created, compiled, sent or received on government information systems are records of the government. These records:

- Are the property of the Government of British Columbia;
- Must be managed in accordance with the Information Management Act and related regulations, policies, standards and procedures; and,
- Are subject to the access and the protection of privacy provisions of the Freedom of Information and Protection of Privacy Act.

Recommended Tests:

Note: 1.2.3 is reported on as part of the annual information security review.

- Demonstrate that employees are aware that electronic information on government systems constitutes a government record.
- Demonstrate that employees are aware of the secure electronic messaging requirements.
- Demonstrate information security classification and labeling is used to identify protection requirements.
- Demonstrate consideration for record management is given when using electronic messaging.
- Demonstrate a Security Threat and Risk Assessment and a Privacy Impact Assessment is completed on all electronic messaging services.

1.2.4	**Security controls must be implemented to mitigate the business and security risks associated with the interconnection of business information systems.** **a) Information in business information systems** **b) Shared directories**

Purpose: ***To restrict access to information in shared business information systems.***

1.2.4 a) Information in business information systems

Information Owners must document and implement procedures to restrict access to information in interconnected internal administrative and productivity information systems that support government such as e-mail, calendars and financial systems.

A Security Threat and Risk Assessment must be conducted to:

- Determine if business information systems provide sufficient protection for the information being shared;
- Define controls to manage information sharing;
- Reduce the risk of social engineering; and,
- Identify access control requirements.

1.2.4 b) Shared directories

The status of employees must be indicated in shared directories (e.g., employee or contractor).

Recommended Tests:

Note: 1.2.4 is not reported on as part of the annual information security review.

- Demonstrate that a Security Threat and Risk Assessment has been completed.

1.2.5 A confidentiality agreement reflecting organizational requirements for the handling of information must be in place and reviewed regularly.
a) Confidentiality agreements

Purpose: ***To ensure employees understand their role in maintaining the confidentiality of information and information systems.***

1.2.5 a) Confidentiality agreements

Information Owners and Information Custodians must:

- Ensure employees are informed of their obligation to maintain the confidentiality of information; and,
- Ensure individuals other than employees accept and sign an agreement to maintain the confidentiality of information.

Confidentiality requirements must be reviewed and updated annually.

Recommended Tests:

Note: 1.2.5 is reported on as part of the annual information security review.

- Demonstrate that a Ministry on-boarding process includes confidentiality agreements.
- Demonstrate that employees are made aware of the requirements to keep confidential information safe from disclosure.