BRITISH COLUMBIA | Ministry of Citizens' Services

Information Security Guidebook for Small and Medium Businesses

The Basics of Information Security

April 2019

CIRMO CSD ES ICT OCIO PSD RPD SBC

Table of Contents

Introduction

Technology has become integrated in today's society in that almost every household in Canada has at least one computing device and computers in some form are part of most workplaces. In only the past several years, software applications and e-business have been widely introduced in the B.C. government to improve the delivery of services and programs to citizens. B.C. government workplaces have been continuously evolving to improve and enhance the ways in which employees and citizens interact. For B.C. government employees, access to the appropriate computing hardware, software and mobile devices has meant ongoing change and continuous learning. Changes have sometimes seemed so rapid and complex that employees have been concerned about learning all they need to know about the technology they now use every day.

Protection of the information in the care of the B.C. government will always be a priority. Citizens must have confidence that the government will protect their personal information and trust government's intention to use that information only as required.

Information security has grown more critical than ever before as technology has become more ubiquitous and more complex. Why? It's due to computer crime by cyber criminals becoming one of the most important issues faced by all organizations and individuals. As new devices, software and applications are introduced, there are computer criminals around the world who work very hard to exploit any vulnerability they can find or create to their advantage.

Businesses that wish to work with government are bound by the terms of the contract and it is their responsibility to ensure that they meet the requirements of the security schedule. This document provides guidance on basic information security controls that small and medium sized businesses should consider to help protect sensitive or critical information assets. Links to documents maintained by the Province are provided as further guidance.

Personnel Security Screening

Personnel security screening helps organizations ensure that they know who they are hiring. The objective is not to invade privacy but to determine if there are any offences on record that are relevant to the duties they will be discharging. For example, if the individual were recently convicted of counterfeiting, the organization may not want to have the individual work in accounts payable or receivable. It is recommended that organizations conduct a criminal record check in addition to a reference check when hiring the individual and require that the individual disclose any offences past, present, or future.

Organizations should work with a reputable organization to conduct a criminal record check on employees to determine whether any relevant crimes are on record.

For more information on personnel security screening please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/criminal-record-checks

Security Awareness Training

Security awareness training helps organizations ensure that employees understand their role in protecting confidentiality of data and know what is expected of them. Organizations should ensure that all employees are required to take an awareness course on a recurring basis that outlines their responsibilities, what resources are available to help, and who to contact with questions.

For more information on security awareness training please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-embedding-dna-controls/security-awareness-program

Information Security Policy

Information Security Policy helps organizations clearly identify how the organization will protect the confidentiality, integrity and availability of data. Organizations should ensure that they have such a policy so that employees know what is and is not acceptable.

A sample information security policy that organizations can update and use is at: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/security-hygiene-controls-from-2016

Security Threat and Risk Assessments

It is essential that organizations conduct risk assessments prior to introducing new systems or making material changes to existing ones.

A sample Security Threat and Risk Assessment template organizations can update and use is at: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/security-hygiene-controls-from-2016

Change Management

In order to maximize availability of services, organizations require robust change management practices. Change management ensures that employees know when and how to initiate controlled changes with planned start and end times, methods of procedure, and testing and back-out plans.

For more information on change management please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-

management-technology/information-security/defensible-security/security-directives/change-management

Backups

Backups are required to recover from unexpected failures of systems affecting data. Attackers are increasingly targeting data for ransom or extortion. Backed up data where the backups have been successfully tested allows organizations to recover from incidents.

For more information on backups and restores please visit:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/backup-and-retention

Business Continuity Plans and Disaster Recovery Plans

Business Continuity Plans and Disaster Recovery Plans are similarly required to recover from unexpected failures of systems. Having a plan is essential to assist with a smooth recovery.

For more information on business continuity plans and disaster recovery plans please visit:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-directives/business-continuity-and-disaster-recovery-plan

Security Incident Response and Management

Security Incident Response and Management are also required to recover from unexpected privacy and security incidents. Preparation and planning in advance is required to ensure incidents are identified, contained, eradicated, and recovered from in an orderly fashion.

A sample Security Incident Response Plan template organizations can update and use is at:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/security-hygiene-controls-from-2016

Encryption

The use of encryption is required to ensure that the information is not readable if it falls into hands of unauthorized users. It enhances confidentiality and significantly reduces the risk of information compromise or a breach. Sensitive information should be encrypted in transit and at rest.

For more information please visit:
https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/cryptographic_standards_v17.pdf

Logical Isolation

Information systems and users should be separated based on the principles of need-to-know and least privilege, risk management and separation of duties. Network configuration, zones and perimeters should be defined based on business requirements and identified risk (e.g., information classification, data flow, potential for malicious traffic, etc.)

For more information please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/logical-access-control

User Identifiers and Access

Users are required to have unique identifiers (user IDs), their activity should be traceable and they should have access only to information and resources required for them to perform their duties. There should be a process for requesting, granting, approving and revoking access. These functions should be separated so that one person cannot be a requestor and an approver at the same time.

For more information please visit:
https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/iss_v1.pdf (Chapter 5)

Authentication

Users are required to verify their identity using an authentication mechanism (e.g., a combination of user ID and a password, multi-factor authentication, use of biometrics, etc.) prior to accessing information and information resources. Use of strong passwords (i.e., hard-to-guess) should be enforced and they should not be stored in clear text.

For more information please visit:
https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/iss_v1.pdf (Chapter 5)

Logging

Audit logs are used to record user and system activities, exceptions, and information security and operational events including information about activity on networks, applications and systems – who did what and when. The level of details to be logged should be based on the value or sensitivity of the information or information system. Logs should be retained in accordance with retention schedules and monitored regularly to assist with a timely response to an incident.

For more information please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/logging-and-monitoring

Application Development

Applications should be developed using a secure development process maintaining security throughout the development life-cycle. Adopting security-by-design approach helps bake in security features and functions from the very beginning and results in a secure-smart application.

For more information on secure application development standards please visit: https://www.owasp.org/index.php/Main_Page

Physical Security

People, facilities and equipment should be adequately protected from environmental and man-made threats such as fire, water damage, break-ins, heating, ventilation and air conditioning failure, etc.

For more information please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/physical-security-and-visible-identification

Production Data in Test

Test data should be protected and controlled the same way as the data in the operational system where that data was extracted from. Confidential, sensitive and personal information should not be used as test data.

For more information please visit: https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/iss_v1.pdf (Chapter 10)

System Hardening

System hardening refers to limiting the functionality of a system to a minimum required – removing or disabling unnecessary software, ports, services, functions, changing default passwords, etc.

For more information please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/defence-in-depth-for-endpoints-and-network

Perimeter controls

You need to know what your network boundaries are and what your important assets are to set up safeguards accordingly. Technologies such as anti-virus, encryption, firewalls should be used, as well as technologies to prevent and detect incidents. Information systems should be tested regularly to verify that technical controls are applied in accordance with business and security requirements. Particularly, after making changes to a system, applying updates and

patches it is important to do a technical compliance check to make sure that security controls and safeguards were not inadvertently changed or disabled.

For more information please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/defence-in-depth-for-endpoints-and-network

Application firewall

Application firewalls are used to control, monitor and filter input and output, access to and from an application or a service. It helps protect and manage application communication much like a network firewall does for networks.

For more information please visit: https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/security_standard_application_web_development_deployment.pdf

Management network

Management networks can exist in addition and in parallel to the network that you are trying to manage – a dedicated network that allows your management systems to communicate with the network elements that they are managing.
Security controls should be in place to protect network infrastructure, including network configuration information, information in transit and at rest.

For more information please visit:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/defence-in-depth-for-endpoints-and-network

Remote management and secure access gateway

Remote access technologies allow users to connect to their corporate network from different devices, different locations and on the go. This type of access requires remote user authentication and a secure access gateway technology such a Virtual Private Network (VPN), desktop terminal services or web access.

For more information please visit: https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/iss_v1.pdf (Chapter 5)

Database Security

Databases often contain confidential, sensitive or personal information, which requires a certain level of protection. Security controls and safeguards should be applied based on security classification level, value and sensitivity of the information housed in the database, including controls around user access and permissions.

For more information please visit:
https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/policies-procedures/it-policies/database_security_standards_for_information_protection_-_2018-04_version_1.pdf

Antivirus

Servers, workstations, tablets, and mobile devices are required to have malware protection technologies. Real-time scanning should be enabled to minimize the risk of infection.

For more information please visit:
https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/iss_v1.pdf (Chapter 8)

Vulnerability Management, Scanning, and Patching

To minimize the risk from technical vulnerabilities vendor provided updates and patches should be applied in a timely manner. Scanning tools and utilities can be used to identify vulnerabilities and apply mitigating controls. Only vendor supported software should be used and plans have to be in place to migrate from end-of-life products to alternative solutions.

For more information please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/vulnerability-management-patching

Asset Management and Disposal

An inventory of important information and information technology (IT) assets should be documented and maintained. Asset inventory should include such information as name, description, number, where applicable security classification, owner, etc. It helps to track where information exists and what level of protection it may require, what to do when assets are lost or stolen, as well as how and when it should be disposed of.

For more information please visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-directives/asset-management

Investigations

All suspected fraudulent activities or inappropriate use of information resources should be reported following an established process. Any misuse or abuse of information resources should be investigated according to standard investigation techniques. The process should be documented and communicated – including reporting requirements, requirements for conducting investigation and collection of evidence, and final resolution.

For more information please visit:
https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/iss_v1.pdf (Chapter 12)

Reference Guide to Many of the Policies Related to Information Security

Appropriate Use Policy:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/appropriate-use-policy

Defensible Security https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security

Security Hygiene Controls from 2016:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/security-hygiene-controls-from-2016

Information Security Policy:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/information-security-policy

Information Incident Management Process:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents

General Incident or Loss Report (GILR) Online Report Form: http://gilr.gov.bc.ca/

Working Outside the Workplace Policy, the Home Technology Assessment Form and How to Protect Your Home Computer:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/working-outside-workplace

IM/IT Standards https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard

Additional Resources

Office of the Chief Information Officer:
http://www2.gov.bc.ca/gov/content/governments/organizational-structure/ministries-organizations/central-government-agencies/office-of-the-chief-information-officer (external) and https://intranet.gov.bc.ca/thehub/ocio (internal)

Information Security: http://www.gov.bc.ca/informationsecurity (external) and https://intranet.gov.bc.ca/thehub/ocio/ocio-enterprise-services/information-security-branch (internal)

Legislation, Privacy and Policy Branch (for privacy legislation and information):
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy

Ministry Information Security Officers (MISOs)
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/information-security-policy/role-of-miso

Security News Digest is a compilation of global news stories about current security breaches, threats, and research, and is available online at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

Appendix A – Definitions

"Device" means any device to manage, operate or provide the Services or to connect to any Systems or any Province system or network, or that is capable of storing any Protected Information, and includes any workstation or handheld device the Contractor authorizes Personnel to use in relation to this Agreement.

"Facilities" means the physical locations (excluding those of the Province) the Contractor uses to provide the Services, or to house Systems or records containing Protected Information.

"Least Privilege" means the principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks so as to limit the damage that can result from accident, error or unauthorized use.

"Need-to-Know" means the principle where access is restricted to authorized individuals whose duties require such access and not merely because of status, rank or office.

"Personnel" means all individuals hired or used by the Contractor and Subcontractors to perform the Contractor's obligations under this Agreement, including unpaid volunteers and the Contractor or a Subcontractor if an individual.

"Policies" means the intentions and directions of an organization or part of it, as expressed in record form by its top management (including, for example, policies, directions, standards, practices, procedures and guidelines).

"Protected Information" means any and all "personal information" as defined in the Privacy Protection Schedule if attached; information and records of information the Contractor is required to treat as confidential under this Agreement; and records, the integrity or availability of which are to be preserved by the Contractor under this Agreement, which in the case of records not falling within (i) or (ii), are marked or instructed by the Province to be so preserved or otherwise treated as "Protected Information" under this Agreement.

"Security Event Logs" means any logs (also known as audit records) of events, notifications or alerts that any component of any Device or other device (not limited to security device), or any Systems or other system or software is technically capable of producing in relation to its status, functions and activities that may be used for such purposes as security investigations, auditing, monitoring and determining security incidents (examples of components capable of producing such logs include firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, networks, authentication services, directory services, dynamic host configuration protocols, dynamic naming services, hardware platforms, virtualization platforms, servers, operating systems, web servers, databases, applications, application firewalls).

"Systems" means any systems, subsystems, equipment, infrastructure, networks, management networks, servers, hardware and software the Contractor uses in relation to this Agreement, including for managing, operating or providing the Services, but excluding any the Province owns or makes available to the Contractor for the Contractor to use in relation to this Agreement.

"Tenancy" means those components of the Systems that directly access and store Protected Information, relate to Protected Information or the Province's tenancy activities, or are customer facing and managed by the Province in its use of the Services.

"Tenancy Security Event Logs" means Security Event Logs that relate to Tenancy, including log-on/log-off information about Province user activities, and application logs, web server log, file server logs, database logs of applications, web servers, file servers or database servers or any other logs that directly store, access or contain Protected Information.