CAN/CIOSC 104:2021
NATIONAL STANDARD OF CANADA

Baseline cyber security controls for small and medium organizations

03.100.01; 35.030

- Page left intentionally blank -

Table of Contents

- Page left intentionally blank -

Foreword

CIO Strategy Council (CIOSC) is not-for-profit corporation providing a national forum for public and private sector members to transform, shape and influence the Canadian information and technology ecosystem.

CIOSC standards are developed in accordance with the *Requirements & Guidance – Accreditation of Standards Development Organizations*, 2019-06-13, established by the Standards Council of Canada (SCC).

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. CIOSC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of this Standard are included in the Introduction.

For further information about CIOSC, please contact:

CIO Strategy Council
1000 Innovation Dr., Suite 500
Ottawa, ON K2K 3E7
ciostrategycouncil.com

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

- Page left intentionally blank -

Introduction

This is the First Edition of CAN/CIOSC 104:2021, Baseline cyber security controls for small and medium organizations.

CAN/CIOSC 104:2021 was prepared by the CIO Strategy Council Technical Committee 5 (TC 5) on cyber security, comprised of over 140 thought leaders and experts in cyber security and related subjects. This Standard was approved by a Technical Committee formed balloting group, comprised of 3 producers, 3 government / regulator / policymakers, 3 users, and 3 general interests.

All units of measurement expressed in this Standard are in SI units using the International system (SI).
This Standard is subject to technical committee review beginning no later than one year from the date of publication. The completion of the review may result in a new edition, revision, reaffirmation or withdrawal of the Standard.

The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the user of the Standard to judge its suitability for a particular application.

This Standard is intended to be used for conformity assessment.

How to use this document

Ideally, organizations invest in cyber security to balance their individual cyber security risks and business objectives. However, as smaller sized organizations lack the resources to develop customized cyber security plans, this Standard outlines security controls which (when implemented) can serve as a cyber security baseline for these organizations.

The requirements in this document are broken down into two categories: “Level 1 and Level 2”.

Level 1 requirements are intended for smaller organizations that are just starting their cyber security journey. These organizations typically do not have the resources to invest in or outsource IT resources and their knowledge of cyber security would be considered entry-level.

Level 2 requirements are intended to build from Level 1 requirements as organizations mature and develop their cyber posture. Organizations adopting Level 2 requirements will have implemented Level 1 requirements, have a basic understanding of cyber security, general knowledge of the cyber related risks they face, and are looking to increase their cyber security maturity.

ICS 03.100.01; 35.030

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

- Page left intentionally blank -

Baseline cyber security controls for small and medium organizations

1 Scope

This Standard specifies a minimum set of cyber security controls intended for small and medium organizations which typically have less than 500 employees.

NOTE 1: Organizations with more than 500 employees may also benefit from leveraging this standard as a starting point to improve their cyber security posture. They will have to evaluate whether their unique situations warrant additional cyber security investments or not.

NOTE 2: Organizations (regardless of size) that handle personally identifiable information, financial, sensitive, or private information, have high-availability requirements of their systems or supply into high-risk sectors (such as critical infrastructure or military) may require additional cyber security controls and requirements beyond the scope of this document. Each organization would need to make this evaluation for themselves.

NOTE 3: While it is encouraged that organizations always consider physical security as a key aspect of their cyber security program, given the complexity and resources required, it is out of scope of this Standard.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Open Web Application Security Project (OWASP) Top 10 Vulnerabilities

Payment Card Industry, Data Security Standard (PCI DSS).

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

application system failure
an incident affecting the confidentiality, integrity, or availability of applications.

biological or behavioural characteristic confirmation
an identity verification method that uses biological (anatomical and physiological) characteristics (e.g., face, fingerprints, retinas) or behavioural characteristics (e.g., keyboard stroke timing, gait) to prove that the person presenting the identity information is the valid owner of the identity.

NOTE: Biological or behavioural characteristic confirmation is achieved by means of the challenge-response model: the biological or behavioural characteristics recorded on a document or in a data store are compared to the person presenting the identity information.

[SOURCE: CAN/CIOSC 103-1:2020]

confidentiality
the ability to protect sensitive information from access by unauthorized people.

consequential service
services that affect human well being such as finance, aid (or assistance), housing, education, recruiting, entitlements.

cyber security incident
any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.

data breach
a *cyber security incident* wherein someone takes sensitive information without the authorization of the owner.

denial of service
see “service interruption”.

DMARC
(domain-based message authentication, reporting & conformance) is an email authentication protocol. It is designed to given email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing.

domain name system (DNS)
hierarchical, distributed global naming system used to identify entities connected to the Internet

NOTE: The Top-Level Domains (TLDs) are the highest in the hierarchy.

[SOURCE: ISO/TR 14873:2013]

encryption
converting information from one form to another to hide its content and prevent unauthorized access.

[SOURCE: Canadian Centre for Cyber Security]

enterprise mobility management
systems that manage movable computing devices or services for an enterprise.

firewall
a security barrier placed between two perimeters that controls the amount and kinds of traffic that may pass between the two.

injury
the damage that businesses suffer from the compromise of information systems and IT assets.

Incident response plan
is a document that establishes processes, procedures, and documentation related to how your organization detects, responds to, and recovers from incidents. Cyber threats, natural disasters, and unplanned outages are examples of incidents that will impact your network, systems, and devices.

[SOURCE: Canadian Centre for Cyber Security]

integrity
the ability to protect information from unauthorized modification or deletion.

IT
information technology.

least privilege
The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.

[SOURCE: Canadian Centre for Cyber Security]

loss of Information
see “unauthorized disclosure”.

malicious code
programs or code written for the purpose of gathering information about systems or users, destroying system data, providing a foothold for further intrusion into a system, falsifying system data and reports, or providing time-consuming irritation to system operations and maintenance personnel.

NOTE 1: Malicious code attacks can take the form of viruses, worms, Trojan horses, or other automated exploits.

NOTE 2: Malicious code is also often referred to as “malware”.

[SOURCE: IEC/TS 62443-1-1:2009]

malware
malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

[SOURCE: Canadian Centre for Cyber Security, Glossary]

may
a keyword that indicates flexibility of choice with implied preference.

multi-factor authentication
authentication that uses a combination of two or more different authentication factors – something a user knows (e.g. a password), has (e.g. a physical token), or is (e.g. a biometric) – to verify a user's identity.

network system failures (widespread)
an incident affecting the confidentiality, integrity, or availability of networks.

OWASP
open web application security project.

password manager
A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services. A password manager assists in generating and retrieving complex passwords, storing such passwords in an encrypted database, or calculating them on demand.

patching
the act of applying updates to computer software or firmware.

privacy breach
incident that involves real or suspected loss of personal information.

ransomware
a type of *malware* that denies a user's access to a system or data until real or virtual goods and/or funds are paid.

sensitive information
information that requires protection against unauthorized disclosure.

secure mobility
security of mobile devices e.g. cellular phones and tablets.

secure portable media
security of portable media devices e.g. USB flash drives.

service interruption
incident that prevents access to a service or otherwise impairs normal operation.

shall
a requirement for test methods specifications or implementations.

should
a keyword indicating flexibility of choice with a strongly preferred alternative; equivalent to the phrase "it is strongly recommended".

unauthorized access
access to physical or logical network, system, or data without permission.

unauthorized disclosure
an incident affecting the confidentiality, integrity, or availability of data.

unauthorized use
use of a physical or logical network, system, or data without permission.

virtual private network (VPN)
restricted-use logical computer network that is constructed from the system resources of a physical network by using encryption and/or by tunnelling links of the virtual network across the real network.

[SOURCE: ISO/IEC 18028-3:2005]

wireless local area networking (WLAN)/(Wi-Fi)
wireless local area networking technology that allows electronic devices to network, mainly using the 2,5 GHz and 5 GHz radio bands.

NOTE 1: "Wi-Fi" is a trademark of the Wi-Fi Alliance.

NOTE 2: "Wi-Fi" is generally used as a synonym for "WLAN" since most modern WLANs are based on these standards.

[SOURCE: ISO/IEC 27033-6:2016]

wi-fi protected access
security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks.

[SOURCE: ISO 20415:2019]

4 Organizational controls

4.1 Leadership

4.1.1 Context

4.1.1.1 Top management of the organization is ultimately responsible for the cyber security program.

4.1.2 Level 1 requirements

4.1.2.1 Top management shall demonstrate their commitment to the cyber security program by:

a. ensuring the cyber security policy and objectives are established and are aligned with the strategic direction of the organization;

b. ensuring that the resources needed for the cyber security program are available and are aligned with the cyber security policy and objectives;

c. communicating the importance of effective cyber security and of conforming to the cyber security program requirements;

d. establishing cybersecurity program metrics and tracking progress; and

e. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

4.1.3 Level 2 requirements

4.1.3.1 For this section all requirements are considered Level 1.

4.2 Accountability

4.2.1 Context

4.2.1.1 Top management of the organization is responsible for clearly defining roles and responsibilities that are essential to the implementation of the baseline cyber security controls.

4.2.2 Level 1 requirements

4.2.2.1 For this section, all requirements are considered Level 2.

4.2.3 Level 2 requirements

4.2.3.1 Top management shall appoint a member of the senior-level leadership team to oversee and be accountable for the organization's IT security. Accountabilities of the member of the senior-level leadership team shall include the following:

a. developing and implementing a company-wide information cyber security program to meet baseline cyber security controls;

b. documenting and disseminating information security policies and procedures;

c. coordinating the development and implementation of a company-wide information security training and awareness program;

d. coordinating a response to actual or suspected breaches in the confidentiality, integrity, or availability of the organization's data; and

e. identifying organizational risks and prioritizing risk treatment relative to likelihood and potential impact of cyber threats.

4.3 Cyber security training

4.3.1 Context

4.3.1.1 Human error while using information systems remains a pivotal element of many cyber security incidents.

4.3.2 Level 1 requirements

4.3.2.1 The organization shall train employees on basic security practices, including a focus on the following practical and easily implementable measures:

a. The use of effective password policies (see Subsection 5.5);

b. Identification of malicious emails and links;

c. Use of approved software;

d. Appropriate usage of the Internet; and

e. Safe use of social media;

4.3.3 Level 2 requirements

4.3.3.1 The organization shall invest in regular and ongoing cyber security awareness and training for their employees.

4.4 Cyber security risk assessment

4.4.1 Context

4.4.1.1 A cyber security risk assessment forms part of an organization's framework to identify, understand, prioritize, and manage cyber security risk to their systems and data assets. It supports an organization in determining potential injury to the confidentiality, integrity, and availability of their systems and data assets.

4.4.1.2 A cyber security risk assessment assists an organization with identifying threats and vulnerabilities of concern and in establishing appropriate security controls to ensure uninterrupted delivery of services.

NOTE: The organization may perform the cyber security risk assessment themselves or outsource to a third-party.

4.4.2 Level 1 requirements

4.4.2.1 Complete the “Cyber Security Risk Assessment Questionnaire” found in Annex B.

4.4.3 Level 2 requirements

4.4.3.1 The member of the senior-level leadership team appointed to oversee the organization’s IT security shall conduct cyber security risk assessments and coordinate the implementation of cyber security controls to address potential cyber security risks.

NOTE 1: The member of the senior-level leadership team appointed to oversee the organization’s IT security should consult experts to review and provide input into the cyber security risk assessment and in the selection of controls to safeguard against cyber security risks identified and assessed.

NOTE 2: The organization may consider the implementation of physical controls as part of its framework to mitigate cyber security risks.

4.4.3.2 The organization shall develop and maintain a list of their information systems and assets. For any information systems and assets not included in their implementation of the baseline cyber security controls, the organization shall document all instances where they make the business decision not to do so.

4.4.3.3 Cyber security risks accepted by the organization shall be documented and authorized by a senior official of the organization.

4.4.3.4 The organization shall identify their financial spending levels for IT and IT security investment (as raw numbers and as a percent of total expenditures).

4.4.3.5 The organization shall identify their internal staffing levels for IT and IT security (as raw numbers and as a percent of total staff).

4.4.3.6 The organization shall commit to progressive improvements to cyber security.

4.4.3.7 The organization shall determine triggers and thresholds to conduct a new or update an existing cyber security risk assessment.

4.4.3.8 Regardless of the outcomes from the cyber security risk assessment, the organization shall implement the foundational or baseline cyber security controls specified in Section 5, and as appropriate, Section 6 based on its business environment.

4.4.3.9 The organization shall periodically review and/or test cyber security controls to ensure effectiveness. Testing and/or review shall take place at a minimum annually, or if a major change occurs in their system.

5 Baseline controls

5.1 Incident response plan

5.1.1 Context

5.1.1.1 Incident response plans ensure organizations are prepared to manage security incidents in an effective and efficient manner. This section describes a model plan for responding to security incidents within an organization. It identifies the structure, roles and responsibilities, types of common incidents, and the approach to preparing, identifying, containing, eradicating, recovering, and conducting a lessons learned analysis in order to minimize impact of security incidents.

The organization may request the services of a managed services provider (MSP) or other qualified external party to support the implementation of the organization's incident response plan.

5.1.2 Level 1 requirements

5.1.2.1 The organization shall have an incident response plan for how to respond to incidents of varying severity. If an organization is unable to manage some types of incidents on its own, the organization should have a plan for what it will do.

5.1.2.2 The incident response plan shall detail who is responsible for handling incidents including any relevant contact information for communicating to external parties, stakeholders and regulators. The organization shall have an up-to-date hard copy version of this plan available for situations where soft copies are not available.

NOTE: The organization should define a method to contact affected parties (internal and external) in case of an incident.

5.1.2.3 The organization should consider purchasing a cyber security insurance policy that includes coverage for incident response and recovery activities or provide rationale for not purchasing one.

5.1.2.4 The organization may use the incident response plan template (see Annex A) as a measure of satisfying Requirements contained in Subsection 5.1.2.

5.1.2 Level 2 requirements

5.1.2.1 For this section, all requirements are considered Level 1.

5.2 Automatically patch operating systems and applications

5.2.1 Context

5.2.1.1 IT vendors release software and firmware updates (patches) on a regular basis to address

defects and security vulnerabilities. Manually keeping track of what vulnerabilities exist for various products located across a network is time-consuming and expensive. At the large organization level, the costly but effective practices of vulnerability and patch management reduce cyber security risks.

5.2.1.2 Small and medium organizations can enable automatic updates for all software and hardware if such an option is available – or consider replacing products with ones that provide the option. This includes replacing software and hardware that no longer receive updates because the vendor ended support (i.e., products past their end of life). This will keep standalone devices, operating systems, applications, and security software up-to-date and free of known vulnerabilities.

5.2.2 Level 1 requirements

5.2.2.1 The organization shall have up-to-date security patches for all software and hardware installed to protect assets from known vulnerabilities.

5.2.2.2 The organization shall enable automatic patching for all software and hardware or document all instances where they make the business decision not to do so.

NOTE 1: This includes all servers, laptops, desktops, tablets, mobile phones and network equipment products.

NOTE 2: The organization should have a business process to ensure regular manual updates for software and hardware that are not capable of automatic updates.

NOTE 3: The organization may establish a testing procedure to ensure patches do not cause a disruption to business functions if a risk analysis determines that such a capability is a sensible risk reduction measure.

5.2.2.3 The organization shall perform a risk assessment whether to replace systems incapable of automatic patching.

5.2.3 Level 2 requirements

5.2.3.1 For this section, all requirements are considered Level 1.

5.3 Enable security software

5.3.1 Context

5.3.1.1 Organizations can protect themselves against the threat posed by known malware (e.g. viruses, worms, Trojan horses, ransomware, spyware) by securely configuring and enabling anti-virus and anti-malware software as feasible on all connected devices.

NOTE: Organizations may activate any software firewalls included on the devices that are within organizational networks. Alternatively, organizations may install and configure a

comparable alternative to achieve the same result.

5.3.2 Level 1 requirements

5.3.2.1 The organization shall enable anti-malware solutions that update automatically and prevent malware from executing without user intervention.

5.3.3 Level 2 requirements

5.3.3.1 For this section, all requirements are considered Level 1.

5.4 Securely configure devices

5.4.1 Context

5.4.1.1 Default administrative passwords and insecure default settings on devices are a significant problem in enterprise networks. Vendors and even resellers often configure devices with default administrative passwords, which often become public.

5.4.1.2 Organizations have the ability to change all administrative passwords on devices. While doing so, organizations can also review device settings (which may be set to insecure defaults) to disable all unnecessary functionality on devices, and to enable any necessary security features. Organizations may want to consider adopting secure product configuration profiles such as the Center for Internet Security Benchmarks – or contracting an IT service provider/MSSP to do so on their behalf.

5.4.2 Level 1 requirements

5.4.2.1 The organization shall implement secure configurations for all their devices by:

a. changing all default passwords.

5.4.3 Level 2 requirements

5.4.3.1 The organization shall implement secure configurations for all their devices unless it is impossible to do so on a specific device:

a. by turning off unnecessary features i.e., block unused ports, disable unused services, remove unused or obsolete software; and

b. by enabling all relevant security features.

5.5 Use strong user authentication

5.5.1 Context

5.5.1.1 Organizations user authentication policies can balance security with usability. Industry best practice is multi-factor authentication which combines the use of something the user knows (e.g. a password) with something that the user has (e.g. a physical token, an app-generated code, an automated phone call to a telephone number on file), or something the user is (e.g. biometric). Not all multi-factor solutions are equal – but all improve an organization's overall cyber security posture.

5.5.2 Level 1 requirements

5.5.2.1 The organization shall implement multi-factor authentication or document all instances where they cannot or make the business decision not to do so.

5.5.2.2 The organization shall enforce password changes on suspicion or evidence of compromise.

5.5.2.3 The organization shall have clear policies on password length and reuse, the use of password managers and if, when, and how users can physically write down and securely store a password.

NOTE: The organization may use password selection guidance from the Communications Security Establishment's User Authentication Guidance for Information Technology Systems.

5.5.3 Level 2 requirements

5.5.3.1 The organization shall implement a password manager or document the business decision not to do so.

NOTE: Best Practices for Passphrases and Passwords (ITSAP.30.032) - https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

5.6 Backup and encrypt data

5.6.1 Context

5.6.1.1 Data back-ups are a critical piece of the effort to ensure quick recovery not only from cyber security incidents such as ransomware or malware but also from natural disasters, equipment failures, or theft.

5.6.1.2 Back-ups are also useful in situations where you are unable to access your current systems or if you believe that your data/information has been tampered with.

5.6.2 Level 1 requirements

5.6.2.1 The organization shall determine on a case-by-case basis what business information and software (including but not limited to sensitive information) is essential to the functioning of the organization, and how frequently this information changes.

NOTE: As an example, critical workstations and servers may require daily incremental back-ups, whereas desktops may be recovered from one common image.

5.6.2.2 The organization shall determine on a case-by-case basis what systems to back up and at what frequency since every system will have different back-up and recovery requirements.

5.6.2.3 The organization shall backup systems that contain essential business information and ensure that recovery mechanisms effectively and efficiently restore these systems from backups.

5.6.2.4 The organization shall store backups at a secure offsite location (either physically or via network separated cloud services) at regular intervals to provide diversity in the event of a disaster (fire, flood, earthquake or localized cyber security incident).

5.6.2.5 The organization should consider the use of encrypted backups with securely stored and recoverable key material. Decryption keys and/or unencrypted backups should be stored securely and should be accessible only to authorized employees or officers.

5.6.3 Level 2 requirements

5.6.3.1 The organization shall use a sampling of backup data to test and verify recovery procedures at regular intervals to ensure the integrity of the end-to-end backup and restoration process.

5.7 Establish basic perimeter defences

5.7.1 Context

5.7.1.1 Networks connected to the Internet require protection from online threats through the use of firewalls. A firewall is a software or a hardware device that monitors the flow of traffic and can defend an internal network from outside intrusions. Domain Name System (DNS) firewall solutions prevent connections to known malicious web domains. Solutions are available to protect all devices connected to a corporate network.

5.7.2 Level 1 requirements

5.7.2.1 For this section, all requirements are considered Level 2.

5.7.3 Level 2 requirements

5.7.3.1 The organization shall have a firewall placed between two perimeters that controls the amount and kinds of traffic that may pass between the two.

5.7.3.2 The organization should consider implementing a DNS firewall for outbound DNS requests to the Internet.

5.7.3.3 The organization shall activate any software firewalls included on devices within their networks or document the alternative measures in place instead of these firewalls.

5.7.3.4 The organization shall require encrypted connectivity to all corporate IT resources and require VPN connectivity with multi-factor authentication for all remote access into corporate networks.

5.7.3.5 The organization shall use secure Wi-Fi, at a minimum WPA2-AES, preferably WPA2-Enterprise or WPA3-Enterprise, following password requirements in section 5.5.

5.7.3.6 The organization should segment their networks to ensure networks provided to the public/customers are separated (and/or isolated) from the corporate networks.

5.7.3.7 The organization shall ensure the implementation of DMARC on all organization email services.

5.7.3.8 The organization shall ensure email filtering is implemented.

5.8 Implement access control and authorization

5.8.1 Context

5.8.1.1 Operating under the principle of least privilege, where users have only the minimal functionality required to perform their tasks, improves an organization's cyber posture.

5.8.2 Level 1 requirements

5.8.2.1 For this section, all requirements are considered Level 2.

5.8.3 Level 2 requirements

5.8.3.1 The organization shall provision accounts with the minimum functionality necessary for tasks and shall restrict administrator privileges to an as-required basis.

5.8.3.2 The organization shall remove accounts and/or functionality when users no longer require these for their tasks.

5.8.3.3 The organization shall only permit administrator accounts to perform administrative activities (and not user-level activities such as accessing email or browsing the web).

5.8.3.4 The organization should consider the implementation of a centralized authorization control system.

6 Baseline controls by operating environment

6.1 Secure mobility

6.1.1 Context

6.1.1.1 Mobile devices such as cellular phones are essential to most organizations. Organizations need to decide on the ownership model that they wish to have for mobile devices. Organizations typically either provide company-owned personally enabled (COPE) devices or allow employees to bring their own devices (BYOD). In both cases, organizations need to take steps to secure sensitive information and corporate IT infrastructure access from these devices.

6.1.1.2 Many solutions exist to segregate work and personal spaces, including apps, email accounts, contacts, etc., whether mobile devices are business or employee-owned, ranging from using separate apps for work and personal use to native “secure folder” or “locker” functions for sensitive business information. It is important for organizations to determine how to enforce this separation in a manner that balances the organization’s business and security needs.

6.1.1.3 Applications (apps) can greatly enhance the capability and productivity of mobile devices but can also introduce risk. Organizations with more mature IT infrastructure and business processes may choose an enterprise mobility management (EMM) solution that enables enhanced business features as well as improved administration of mobile devices. EMM solutions vary in capability but generally include functions to manage, audit and support mobile devices in the workplace. They may also include the capability to remotely wipe devices.

6.1.2 Level 1 requirements

6.1.2.1 For this section all requirements are considered Level 2.

6.1.3 Level 2 requirements

6.1.3.1 The organization using mobility (i.e., cellphones) shall decide on an ownership model for mobile devices and document the rationale and associated risks.

6.1.3.2 The organization using mobility (i.e., cellphones) shall:

a. require separation between work and personal data on mobile devices with access to corporate IT resources and document the details of this separation;

b. ensure that employees only download mobile device applications (i.e., apps) from the organization’s list of trusted sources;

c. require that all mobile devices store all sensitive information in a secure, encrypted state;

d. consider the implementation of an enterprise mobility management solution for all mobile devices or document the risks assumed to the audit, management, and security functionality of mobile devices by not implementing such a solution;

e. enforce or educate users to:

- disable automatic connections to open networks;
- avoid connecting to unknown Wi-Fi networks;
- limit the use of Bluetooth and NFC for the exchange of sensitive information; and
- use corporate Wi-Fi or cellular data network connectivity rather than public Wi-Fi; and

f. Consider using secure connectivity (VPN, Virtual Desktop etc.) when connecting to public Wi-Fi networks or provide the rationale for not doing so.

6.2 Secure cloud and outsourced IT services

6.2.1 Context

6.2.1.1 Organizations typically rely on outsourced IT service providers or MSPs for services such as their cloud storage and processing needs, the management and/or hosting of their website, and the management of their online payment systems. It is important for organizations to consider their risk tolerance level with the regulations within the legal jurisdictions where their outsourced providers store or use their sensitive information.

6.2.2 Level 1 requirements

6.2.2.1 Organization using cloud applications and/or outsourcing IT services shall evaluate their risk tolerance level with how their outsourced IT providers handle and access their sensitive information.

6.2.3 Level 2 requirements

6.2.3.1 The organization using cloud applications and/or outsourcing IT services shall:

a. require that all their cloud service providers share an AICPA SSAE 18 or equivalent report that states that they achieved Trust Service Principles compliance or provide a documented business case as why they chose not to;

NOTE: The organization determines equivalence to AICPA SSAE 18.

b. evaluate their risk tolerance level with the legal jurisdictions where their outsourced providers store or use their sensitive information;

c. ensure that their IT infrastructure and users communicate securely with all cloud services and applications; and

d. ensure that administrative accounts for cloud services use multi-factor authentication and differ from internal administrator accounts.

6.3 Secure websites

6.3.1 Context

6.3.1.1 Websites can be secured by addressing the Open Web Application Security Project (OWASP) top 10 vulnerabilities. The vulnerabilities included in the top 10 are injection, broken authentication, sensitive data exposure, XML external entities, broken access control, security misconfiguration, cross-site scripting, insecure deserialization, using components with known vulnerabilities and insufficient logging and monitoring.

6.3.1.2 It can be helpful (or required by their customers) for organizations to understand the OWASP Application Security Verification Standard (ASVS) level they need to meet for each of their websites.

6.3.1.3 Meeting ASVS can be included as a contractual requirement for outsourced websites, or organizations should be prepared to invest to meet these IT security requirements for websites developed and operated in-house.

6.3.2 Level 1 requirements

6.3.2.1 For this section, all requirements are considered Level 2.

6.3.3 Level 2 requirements

6.3.3.1 The organization deploying websites shall ensure that their websites address the OWASP top 10 vulnerabilities.

NOTE: For a comprehensive list of vulnerability scanning tools, please visit the “Vulnerability Scanning Tools” page on the OWASP website.

6.3.3.2 The organization shall ensure that they understand the OWASP ASVS level they need to meet for each of their websites.

6.4 Secure portable media

6.4.1 Context

6.4.1.1 Portable media such as portable hard drives, USB flash drives and secure digital (SD) cards are a convenient way to transfer files between devices. However, given their size and portability,

they are prone to loss or theft, potentially causing a data breach and the introduction of malicious files to your network. Since banning their use altogether may be impractical, organizations may limit the use of portable media to commercial encrypted drives provided by the organization. Organizations should consider tools which control their access and monitor files transferred.

6.4.1.2 It is important that organizations maintain strong asset control for all storage devices, including portable media devices. This includes the proper disposal of such media.

6.4.2 Level 1 requirements

6.4.2.1 Organizations using portable media shall mandate the sole use of organization-owned secure portable media.

6.4.3 Level 2 requirements

6.4.3.1 The organization using portable media shall:

a. have strong asset controls for these devices;

b. require the use of encryption on all of these devices; and

c. have processes for the sanitization or destruction of portable media prior to disposal.

6.5 Point of sale (POS) and financial systems

6.5.1 Context

6.5.1.1 It is important that organizations segment PoS terminals and financial systems, isolating them from the Internet and segmenting them from other areas of the corporate network via a firewall to protect their data assets.

6.5.2 Level 1 requirement

6.5.2.1 The organization using point of sale terminals and financial systems shall follow the Payment Card Industry Data Security Standard (PCI DSS).

6.5.3 Level 2 requirements

6.5.3.1 For this section, all requirements are considered Level 1.

6.6 Computer Security Log Management

6.6.1 Context

6.6.1.1 Log collection, analysis and management forms an integral part of good IT practice and is essential for auditing IT security controls and performing incident management. Organizations of all sizes should have a log management policy in accordance with their needs. Some examples of security logs might include a record of user login events, file or data level accesses, device, or user configuration status messages such as installed software and versions, firewall or intrusion detection system logs, and potentially many others.

6.6.2 Level 1 requirements

6.6.2.1 For this section, all requirements are considered Level 2.

6.6.3 Level 2 requirements

6.6.3.1 The organization shall ensure an appropriate understanding of their security logging capabilities and needs and ensure a corresponding log management policy is in place.

NOTE: NIST SP 800-92, “Guide to Computer Security Log Management” describes considerations for Security Log Management and includes examples. Understanding what data is available and what is missing is a key step in defining a good log management and incident.

Annex A
(informative)

A. Incident response plan template

A.1 Scope

A.1.1 This Incident Response Plan applies to all networks, systems, and data, as well as members of the organization including employees and contractors, as well as vendors that access the networks, systems, and data of the organization. Members of the organization who may be called upon to lead or participate as part of the Incident Response Team are to familiarize themselves with this plan and be prepared to collaborate with the goal of minimizing adverse impact to the organization.

A.1.2 This Incident Response Plan assists an organization with establishing incident handling and incident response capabilities and determining the appropriate response for common security incidents that will arise.

A.2 Requirements

A.2.1 Any employees, contractors, consultants, temporary or other workers of the organization and its subsidiaries that become aware of a cyber security incident or of the possibility of a cyber security incident are to take immediate action by immediately informing their immediate supervisor and the appointed member of the senior leadership team overseeing the organizations IT security.

A.2.2. The following information is recorded when reporting a real or possible security incident (i.e., breach):

a. what happened;

b. where the security incident occurred (i.e., in which department);

c. when the security incident occurred;

d. how and when the real or possible security incident was discovered;

e. type of security incident (if known);

f. what equipment or sections of the information technology environment are impacted; and

g. whether any corrective action has already been taken.

A.2.3 The appointed member of the senior leadership team overseeing the organizations IT security verifies the circumstances of the real and/or possible security incident. The security incident or

suspected security incident is reported upon discovery, with the above information completed.

A.2.4 The organization investigates all reports concerning a security incident using the PICERL (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) process or an equivalent process (i.e., security incident handling process):

a. Preparation

i. In addition to a soft copy, the Incident Response Plan is always available in hard copy thus ensuring the Plan is always accessible irrespective of the status of the internal information technology infrastructure.

NOTE: The organization's retention policy addresses requirements and obligations for retaining documents and records and verification controls.

ii. The Incident Response Plan is reviewed and updated on an annual basis or after an incident has occurred.

iii. The appointed member of the senior-level leadership team overseeing the organization's IT security assembles a pre-determined team (i.e., security incident response team) deemed necessary to fulfil the security incident handling process.

iv. The security incident response team is listed in the incident response plan.

v. Any employees, contractors, consultants, temporary or other workers of the organization, including the security incident response team is provided with adequate training to ensure understanding of the security incident handling process and their roles within it.

vi. The appointed member of the senior leadership team overseeing the organization's IT security of the organization schedules annual training drills of security incidents with the security incident response team.

NOTE: This annual training will ensure that members of the security incident response team are familiar with the types of incidents in advance, will be prepared for the known so they may focus on the unknown, and so the plan, team, and tools are all fully tested.

vii. The documentation for the organization's information technology environment is kept up to date and always available such that it is accessible for reference, provides information on dependencies, and contains vendor information.

b. Identification

i. Any employees, contractors, consultants, temporary or other workers of the organization, including the security incident response team familiarizes

themselves with the following security incident types:

- Unauthorized Use or Access
- Service Interruption or Denial of Service
- Malicious Code
- Network System Failures (widespread)
- Application System Failures
- Unauthorized Disclosure or Loss of Information
- Privacy Breach
- Information Security/Data Breach
- Other (i.e., any other incident that affects networks, systems, or data)

ii. The appointed member of the senior leadership team overseeing the organizations IT security determines the severity (see Table 1) of the incident taking into consideration whether a single system is affected or multiple, the criticality of the system(s) affected, whether impacting a single person or multiple, whether impacting a single team or multiple, or impacting the entire organization. The appointed member of the senior leadership team overseeing the organizations IT security overseeing the organization's IT security considers whether a single business area or multiple and the impact of the incident. The appointed member of the senior leadership team overseeing the organizations IT security considers the relevant business context and what else is happening with the business at the time to fully understand the impacts and urgency of remediation.

iii. The appointed member of the senior leadership team overseeing the organizations IT security considers the available information to determine the known magnitude of impact compared with the estimated size along with likelihood and rapidness of spread. The appointed member of the senior leadership team overseeing the organizations IT security determines the potential impacts to the organization whether financial damage or brand and reputational damage or other harms.

NOTE: The security incident may be the result of a sophisticated or unsophisticated threat, automated or manual attack, or may be nuisance/vandalism.

iv. The appointed member of the senior leadership team overseeing the organizations IT security determines whether there is a vulnerability, whether

there is an exploit, whether there is evidence of the vulnerability being exploited, and whether there is a known patch. The appointed member of the senior leadership team overseeing the organizations IT security determines if this is a new threat (i.e., day zero) or a known threat and the estimated effort to contain the problem.

Category	Indicators	Scope
1 – Critical	Data loss, Malware	Widespread and/or with critical servers or data exfiltration
2 – High	Theoretical threat becomes active	Widespread and/or with critical servers or data exfiltration
3 – Medium	Email phishing or active spreading infection	Widespread
4 - Low	Malware or phishing	Individual host or person

Table 1: Severity Matrix

v. The appointed member of the senior leadership team overseeing the organizations IT security prepares a security incident communications plan such that during such an incident all contact information for the organization's staff, the security incident response team, and any relevant third parties, such as cyber security insurance vendors, is readily available.

vi. The appointed member of the senior leadership team overseeing the organizations IT security assesses the situation and determine if a privacy breach has occurred by answering the following two critical questions:

- **Is Personally Identifiable Information involved?** Identify the type of information affected by the incident in order to determine if a breach has occurred.

- **Has an unauthorized disclosure occurred?** Whether it is intentional, inadvertent or as a result of criminal activity, an unauthorized disclosure constitutes a privacy breach.

NOTE 1: If the answer is yes to both questions, a privacy breach has occurred.

NOTE 2: If a privacy breach has occurred, the organization may be required to report the privacy breach to the authority having jurisdiction.

vii. With the definition of Incident Type, Severity, and if a Privacy Breach has occurred or not, the appointed member of the senior leadership team overseeing the organizations IT security now is able to ascertain if a security incident has occurred. If it is concluded that a security incident has occurred, the following requirements of the incident response plan is followed.

viii. The appointed member of the senior leadership team overseeing the organizations IT security immediately assembles the security incident response team to further identify and gather data on the security incident.

ix. The security incident response team triages the security incident and document information gathered and decisions, including but not limited to:

- The original report of security incident, incident type, incident severity, privacy breach identification, and any actions taken;
- Analysis of the precursors and indicators;
- Research the possible matching known security incidents; and
- Any possible identification of actor, mechanism, application, attack vector, or other information which will assist in the containment and eradication of the root cause of the security incident.

c. Containment

i. The security incident response team documents all information gained and actions taken as they take the following actions to contain the security incident:

- Immediately isolate the security incident where possible, via isolation of the impacted infrastructure;
- Determine the source of the security incident, including what vulnerability was exploited;
- Immediately resolve any identified vulnerabilities or implement workarounds to mitigate the system(s) affected;
- Continue impact and damage assessment and confirm the scope of the incident;
- Determine what environment changes have made, such as but not limited to files, connections, processes, accounts, access, etc.; and
- Acquire, preserve, secure and document evidence and preserve chain of custody.

d. Eradication

i. The security incident response team documents all information gained and actions taken as they take the following actions to eradicate the impact of the

security incident:

- Remove all traces of the infection or other incident;
- Identify and mitigate all vulnerabilities which have been identified during the investigation, whether they were exploited within this security incident or not;
- Remove malware, virus, inappropriate material, and other components introduced by the Security Incident. If necessary, utilize backup restore processes to ensure no trace of any malicious code exists within the environment;
- If more devices within the organization environment are discovered to be impacted, ensure to perform the identification steps on the a newly identified examples, then rerun the containment process;
- Continue research and investigation until the full attack vector is understood; and
- Ultimately take all steps necessary to ensure the Security Incident cannot reoccur.

e. Recovery

i. The security incident response team documents all information gained and actions taken as they take the following actions to recover from the impact of the security incident:

- Return affected systems to an operationally ready state, one by one to ensure operation with reduced risk of the security incident reoccurring;
- Monitor each system brought online, and all environment network edge appliances, closely to ensure incident does not re-occur or is not still ongoing;
- Ensure systems are restored from a trusted and clean source;
- Confirm the affected systems are functioning normally; and
- Implement additional monitoring to look for future related activity if necessary.

f. Lessons Learned

i. The appointed member of the senior leadership team overseeing the organizations IT security is responsible for the creation of a follow up security

incident report.

ii. The appointed member of the senior leadership team overseeing the organizations IT security meets with the security incident response team within 2 weeks to hold lessons learned meeting and to review the security incident report. The outcome of the lessons learned meeting include, but not be limited to:

- A walk through and review play-by-play of the security incident report;
- Understanding of how the security incident was detected, by whom, and when;
- Understanding of the scope and severity of security incident;
- Discuss the methods used in containment and eradication of the security incident;
- Identify any opportunities for improvement to better prepare for future security incidents; and
- Ensure accountability to follow up on identified opportunities.

iii. The outcome of the lessons learned meeting are documented and stored with the security incident documentation.

Annex B
(normative)

B. Cyber security risk assessment questionnaire

The following cyber security risk assessment questionnaire is targeted at raising awareness within small and medium organizations. It is not intended to provide feedback or an overall risk score. As stated in section 4.3.2.1 Note 1, The member of the senior-level leadership team appointed to oversee the organization's IT security should consult cyber security experts to review and provide input into the risk assessment and in the selection of controls to safeguard against cyber security risks identified and assessed. For the purposes of this document, a policy is defined as the rules and procedures that need to be followed for all individuals using an organization's IT assets and resources. An answer of NO, for any of the below questions could mean that your organization is at risk.

1. Are all IT and IT security roles and responsibilities clearly outlined in your organization?	YES/NO
2. Does your organization have an incident response plan?	YES/NO
3. Does your organization have cyber insurance?	YES/NO
4. Has your organization assessed the potential injury to the confidentiality, integrity and accessibility of information systems and assets? https://lih-cai.cse-cst.gc.ca/login/index.php	YES/NO
5. Does your organization store or collect confidential data (credit cards, social security numbers, employee information, etc.)?	YES/NO
6. Does your organisation know its responsibilities under the Privacy Act? https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html	YES/NO
7. Has your organization classified the data that is being stored?	YES/NO
8. Does your organization train employees on your cyber security policies and procedures?	YES/NO
9. Does your organization have a company policy for cyber security spending based on the total IT budget?	YES/NO
10. Does your organization provide cyber security training for IT personnel?	YES/NO
11. Is automatic patching turned on where possible?	YES/NO
12. Does your organization have a policy for backing up and encrypting essential business data?	YES/NO
13. Does your organization have a policy for strong user authentication?	YES/NO
14. Does your organization have a policy for access control and authorization?	YES/NO
15. Does your organization have a policy for securing websites?	YES/NO
16. Does your organization have a security policy for mobility?	YES/NO
17. Does your organization have a policy to establish basic perimeter defense?	YES/NO
18. Does your organization rely on third parties for outsourced IT? (e.g. Cloud, SaaS, remote backups, etc.)	YES/NO
19. Does your organization have a policy for outsourced IT services?	YES/NO

20. Does your organization audit the current set of security controls at least once a year?	YES/NO
21. Does your organization perform vulnerability and penetration tests on information systems at least once a year?	YES/NO

Bibliography

[1] CAN/CIOSC 103-1, Digital Trust and Identity – Part 1: Fundamentals.

[2] Canadian Centre for Cyber Security. Baseline Cyber Security Controls for Small and Medium Organizations.

[3] Cyber Essentials UK.

[4] CyberNB.

[5] IEC TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.

[6] ISACA. Cybersecurity Guidance for Small and Medium-Sized Enterprises, 2015.

[7] ISACA. Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises, 2015.

[8] ISO 19731:2017, Digital analytics and web analyses for purposes of market, opinion and social research — Vocabulary and service requirements.

[9] ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity.

[10] ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[11] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements.

[12] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls.

[13] ITSAP.30.032, Best Practices for Passphrases and Passwords.

[14] Open Web Application Security Project. Application Security Verification Standard.

[15] Open Web Application Security Project. Top 10 Vulnerabilities.

[16] National Institute of Standards and Technology (NIST) Cyber Security Framework.

[17] Payment Card Industry. Payment Card Industry Data Security Standard (PCI DSS).

[18] The IASME Governance Standard for Information and Cyber Security.