Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

BASELINE CYBER SECURITY CONTROLS FOR SMALL AND MEDIUM ORGANIZATIONS V1.2

SMALL AND MEDIUM ORGANIZATIONS

TLP:WHITE

Canada

FOREWORD

The *Baseline Cyber Security Controls for Small and Medium Organizations* is an UNCLASSIFIED publication intended for small and medium organizations in Canada that want recommendations to improve their resiliency via cyber security investments. This document is for the public and, as such, has the Traffic Light Protocol (TLP) marking [1][1] of TLP:WHITE.

REVISION HISTORY

Revision	Amendments	Date
1	First release	March 2019
1.1	Second release	June 2019
1.2	Third release - minor updates to clarify control, more detail in Annex B	February 2020

OVERVIEW

This document presents the Canadian Centre for Cyber Security baseline cyber security controls wherein we attempt to apply the 80/20 rule (achieve 80% of the benefit from 20% of the effort) to the cyber security practices of small and medium organizations in Canada.

DISCLAIMER

Readers should not consider any advice and guidance contained within this report as comprehensive and/or all encompassing. All risks related to the cyber security of information technology systems are the responsibility of system owners.

[1] Numbers in square brackets indicate reference material. There is a list of references in the Supporting Content section of this document.

TABLE OF CONTENTS

1 Introduction 4

2 Organizational Controls 5

2.1 Assess Organizational Size 5

2.2 Determine What Information Technology is in Scope 5

2.3 Determine the Value of Information Systems and Assets 5

2.4 Confirm the Cyber Security Threat Level 6

2.5 Confirm Cyber Security Investment Levels 6

3 Baseline Controls 7

3.1 Develop an Incident Response Plan 7

3.2 Automatically Patch Operating Systems and Applications 7

3.3 Enable Security Software 8

3.4 Securely Configure Devices 8

3.5 Use Strong User Authentication 8

3.6 Provide Employee with Awareness Training 9

3.7 Back up and Encrypt Data 9

3.8 Secure Mobility 10

3.9 Establish Basic Perimeter Defences 11

3.10 Secure Cloud and Outsourced IT Services 12

3.11 Secure Websites 12

3.12 Implement Access Control and Authorization 13

3.13 Secure Portable Media 13

4 Summary 14

5 Supporting Content 15

5.1 List of Abbreviations 15

5.2 Glossary 15

5.3 References 16

LIST OF ANNEXES

Annex A Summary of the Baseline Controls 17

Annex B Summary of Version Changes 20

1 INTRODUCTION

This document is for small and medium organizations seeking to improve their resiliency through investment in cyber security. This is part of the response to the need, expressed in the *National Cyber Security Strategy* [2], for the Government of Canada to support small and medium organizations by making cyber security more accessible.

As stated in the *National Cyber Threat Assessment 2018* [3], small and medium organizations are most likely to face cyber threat activity in the form of cybercrime that often has immediate financial or privacy implications. Cyber threat actors target Canadian businesses for their data about customers, partners and suppliers, financial information and payment systems, and proprietary information. Cyber security incidents can also result in reputational damage, productivity loss, intellectual property theft, operational disruptions, and recovery expenses.

We recommend *Annex 4A – Profile 1* of *ITSG-33 Information Technology (IT) Security Risk Management: A Lifecycle Approach* [4] to organizations seeking to reduce their risk to cyber security incidents. This profile is the Canadian specification of controls equivalent to that of the *NIST Cyber Security Framework* [5] or *ISO/IEC 27001:2013* [6]. The reality, however, is that this profile is expensive to implement and beyond the financial and/or human resources means of most small and medium organizations in Canada.

We believe that organizations can mitigate most cyber threats through awareness and best practices in cyber security and business continuity. As such, we believe we can successfully apply the 80/20 rule (achieve 80% of the benefit from 20% of the effort) in the domain of cyber security and achieve concrete gains for the cyber security of Canadians. This document presents a condensed set of advice, guidance, and security controls on how organizations can get the most out of their cyber security investments. We call these the **baseline cyber security controls** (hereafter **baseline controls**).

We encourage organizations to implement as many of these baseline controls as possible, and we understand that not every organization can implement every control. If the majority of Canadian organizations implement these controls, however, Canada will be more resilient and cyber-secure. For additional advice, please visit cyber.gc.ca.

2 ORGANIZATIONAL CONTROLS

Cyber security depends on a multitude of factors, and as such, it is different for each organization. The goal of this section is to help an organization determine whether the baseline controls are appropriate for its circumstances.

2.1 ASSESS ORGANIZATIONAL SIZE

We intend the baseline controls for organizations that meet the Innovation, Science, and Economic Development Canada definitions of small or medium organizations [7], namely organizations that have less than 500 employees. We recommend that larger organizations should invest in more comprehensive cyber security measures.

To summarize:

OC.1 Organizations using the baseline controls should have less than 500 employees.

2.2 DETERMINE WHAT INFORMATION TECHNOLOGY IS IN SCOPE

Organizations should determine what elements of their information systems and assets are within the scope they wish to consider for the baseline controls. Information systems and assets in this context refer to all computers, servers, network devices, mobile devices, information systems, applications, services, cloud applications, etc. that an organization uses to conduct its business. We strongly recommend that organizations consider all of their information systems and assets, (whether owned, contracted, or otherwise used) within the scope for the baseline controls.

To summarize:

OC.2 Organizations should list which parts of their information systems and assets are in scope for their implementation of the baseline controls and should provide the rationale for excluding information systems and assets and recognize the acceptance of risk in doing so.

2.3 DETERMINE THE VALUE OF INFORMATION SYSTEMS AND ASSETS

Organizations should ensure that they understand the value of their information systems and assets. For example, sensitive information about customers may require protection, as might proprietary intellectual property that makes the organization competitive.

Organizations should assess the injury level related to the confidentiality, integrity, and availability of information systems and/or data:

- For confidentiality, this injury would occur if there was an unauthorized disclosure of sensitive information (e.g. if someone disclosed sensitive information publically or to a competitor).
- For integrity, this injury would occur if there was an unauthorized modification of information (e.g. if someone modified sensitive information to be incorrect).
- For availability, this injury would occur if the information was either unavailable for use for a period or lost permanently (e.g. if someone took down an organization's website or deleted sensitive information).

Organizations should assess the potential injury to the confidentiality, integrity, and availability to their information systems and assets using the following scale:

- Very low – no expected injury
- Low – injury expected (e.g. some financial loss)
- Medium – serious injury expected (e.g. reduced competitiveness, loss of reputation)
- High – extremely grave injury expected (e.g. ongoing viability compromised)

We intend the baseline security controls for situations where all injuries are at or below the medium level. We recommend that organizations with higher potential injuries invest in more comprehensive cyber security measures.

To summarize:

OC.3 Organizations should assess the potential injury to the confidentiality, integrity, and availability to their information systems and assets.

2.4 CONFIRM THE CYBER SECURITY THREAT LEVEL

The *National Cyber Threat Assessment 2018* [3] judges that cybercrime is the cyber threat most likely to affect Canadian small and medium organizations. We designed the baseline controls to be effective for this threat.

There may be situations for small and medium organizations where the cyber security threat exceeds the level of cybercrime. For example, organizations in strategic sectors of the economy should consult the *National Cyber Threat Assessment 2018* [3] and decide if they possess intellectual property or other sensitive information that might warrant commercial espionage against them. Organizations should also decide if cyber security incidents against their information systems and assets have the potential to compromise public and/or national security. We recommend that organizations facing any of these more advanced cyber security threat levels invest in more comprehensive cyber security measures.

To summarize:

OC.4 Organizations should self-identify their primary cyber threat.

2.5 CONFIRM CYBER SECURITY INVESTMENT LEVELS

Organizations should identify someone in a leadership role who is specifically responsible for their IT security. We recommend that larger organizations consider hiring a chief information security officer (CISO).

Organizations should assess their cyber security investment by identifying their expenditure levels towards information technology and IT security. Industry analysis [8] indicates that organizations typically spend up to 13% of their IT budget on cyber security, and recommends that organizations expend 4-7% of their IT budget on cyber security. We recommend that organizations consider their spending in comparison with these figures, but also factor in organizational spending priorities. Organizations should commit to progressive improvements to cyber security. We further recommend that organizations with significant expenditures in IT and IT security invest in more comprehensive cyber security measures.

Note that expenditure levels for IT and IT security include all costs related to IT including outsourcing.

To summarize:

OC.5.1 Organizations should identify someone in a leadership role who is specifically responsible for their IT security.

OC.5.2 Organizations should identify their financial spending levels for IT and IT security investment (as raw numbers and as a percent of total expenditures).

OC.5.3 Organizations should identify their internal staffing levels for IT and IT security (as raw numbers and as a percent of total staff).

OC.5.4 Organizations should commit to progressive improvements to cyber security.

3 BASELINE CONTROLS

In the sections that follow, we introduce the baseline controls to help organizations reduce the risk of cyber security incidents and data breaches. These controls focus on not only reducing risk but also how an organization will respond to such incidents. We recommend that organizations adopt the thinking that they will suffer a data breach at some point and thus be in a position to detect, respond, and recover.

3.1 DEVELOP AN INCIDENT RESPONSE PLAN

Organizations should assume that cyber security incidents will occur and have a plan on how to respond and recover from them. This plan should be part of the organization's plans for disaster recovery and business continuity.

We recommend that organizations establish solutions for detecting, monitoring, and responding to incidents, typically via *security information and event management* systems. Smaller organizations, however, may not have the capacity to perform such activities either in-house or via contracted services. In all cases, organizations should know who responds to an incident and what they are responsible for during it. We recommend that organizations include in these responsibilities any of their legal obligations for reporting cyber security incidents. Organizations that require external assistance when dealing with incidents should have a detailed plan for who to engage and for what services. Organizations should consider purchasing a cyber security insurance policy that includes coverage for incident response and recovery activities in addition to liability coverage.

To summarize:

BC.1.1 Organizations should have a basic 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.

BC.1.2 Organizations should have a written incident response plan that details who is responsible for handling incidents, including any relevant contact information for communicating to external parties, stakeholders, and regulators. Organizations should have an up-to-date hard copy version of this plan available for situations where soft copies are not available.

BC.1.3 Organizations should consider purchasing a cyber security insurance policy that includes coverage for incident response and recovery activities OR provide a rationale for not purchasing one.

3.2 AUTOMATICALLY PATCH OPERATING SYSTEMS AND APPLICATIONS

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.

For small and medium organizations, we recommend that organizations 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.

Note: These recommendations differ from large enterprise recommendations, where we advocate for full vulnerability and patch management. There are inherent risks in automatically patching, namely that there may be unexpected side effects. We believe that smaller organizations can achieve the same cyber security outcome as large organizations by simply accepting the risks of patching by default. This assumption of risk makes less sense in larger organizations who have the staffing to manage and mitigate these risks. Organizations should assess this trade-off on a case-by-case basis.

To summarize:

BC.2.1 Organizations should enable automatic patching for all software and hardware OR establish full vulnerability and patch management solutions.

BC.2.2 Organizations should conduct risk assessment activities as to whether to replace any software and hardware that are not capable of automatic updates. If the organization chooses to keep such devices, they should have a business process to ensure regular manual updates.

3.3 ENABLE SECURITY SOFTWARE

Organizations should 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. Following section 3.2, organizations should configure these applications for automatic updates and scans, and consider replacing any products that lack either of these features.

Organizations should activate any software firewalls included on the devices that are within organizational networks, unless the organization installs and configures a comparable alternative.

To summarize:

BC.3.1 Organizations should enable anti-malware solutions that update and scan automatically.

BC.3.2 Organizations should activate any software firewalls included on the devices that are within organizational networks OR document the alternative measures in place instead of these firewalls.

3.4 SECURELY CONFIGURE DEVICES

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.

Organizations should ensure that they change all administrative passwords on devices. While doing so, organizations should 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* [9] – or contracting an IT service provider to do so on their behalf.

To summarize:

BC.4.1 Organizations should implement secure configurations for all their devices changing all default passwords, turning off unnecessary features, and enabling all relevant security features.

3.5 USE STRONG USER AUTHENTICATION

Organizations should have user authentication policies that balance security with usability. Whenever possible, use two-factor authentication. These methods combine 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). Not all two-factor solutions are equal – but all improve an organization's overall cyber security posture.

We recommend only changing passwords when there is suspicion or evidence of a security issue such as the accidental disclosure of a password or evidence that someone compromised an account.

Organizations should have clear policies on password length and reuse, the use of password managers, and the conditions that a user must meet to physically write down and store a password. We recommend that organizations follow our password selection guidance from *User Authentication Guidance for Information Technology Systems* [10].

To summarize:

BC.5.1 Organizations should implement two-factor authentication wherever possible, and document all instances where they make the business decision not to do so. Organizations should require two-factor authentication for important accounts such as financial accounts, system administrators, cloud administration, privileged users, and senior executives.

BC.5.2 Organizations should enforce password changes on suspicion or evidence of compromise.

BC.5.3 Organizations should 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.

3.6 PROVIDE EMPLOYEE WITH AWARENESS TRAINING

Human error while using information systems remains an element of too many cyber security incidents. As a first line of defence, organizations should train employees on basic security practices. Organizations should focus on practical and easily implementable measures such as the:

- Use of effective password policies (see section 3.5);
- Identification of malicious emails and links;
- Use of approved software;
- Appropriate usage of the Internet; and
- Safe use of social media.

To summarize:

BC.6.1 Organizations should invest in cyber security awareness and training for their employees.

3.7 BACK UP AND ENCRYPT DATA

We recommend that organizations back up all essential business information regularly to an external secure location. 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.

Organizations should determine what business information (including but not limited to sensitive information) is essential to the functioning of the organization, and how frequently this information changes. Organizations should 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. For example, critical workstations and servers may require daily incremental back-ups, whereas desktops may be recovered from one common image.

Organizations should have clear procedures on how to restore from back-ups and regularly verify that back-up and restore mechanisms operate as expected.

Organizations should ensure that they store back-ups in a secure, encrypted state. Back-ups should only be accessible to those responsible for the testing and/or use of restoration activities. Organizations should also consider storing back-ups offsite (either physically or via cloud services) to provide diversity in the event of a disaster (fire, flood, earthquake or localized cyber security incident).

To summarize:

BC.7.1 Organizations should back up systems that contain essential business information and ensure that recovery mechanisms effectively and efficiently restore these systems from back-ups. Organizations should consider storing backups offline at a secure offsite location OR provide the rationale for not doing so.

BC.7.2 Organizations should securely store back-ups in an encrypted state and restrict access to them to those who must access them for the testing or use of restoration activities. Long term backups (e.g. weekly backups) must be stored offline, but frequent backups (e.g. daily backups) may be stored online.

3.8 SECURE MOBILITY

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.

Whether mobile devices are business or employee-owned, a governing principle should be that there exists a separation between work and personal data on these devices, including apps, email accounts, contacts, etc. Many solutions exist to segregate work and personal spaces, ranging from using separate apps for work and personal use to native "secure folder" or "locker" functions for sensitive business information. Organizations should determine how to enforce this separation in a manner that balances the organization's business and security needs. Organizations should require that all mobile devices store all sensitive information in a secure, encrypted state.

We recommend that organizations follow the secure configuration practices of section 3.4 for all mobile devices.

Applications (apps) greatly enhance the capability and productivity of mobile devices but can also introduce risk. To minimize these risks, organizations should require that employees only download apps from trusted sources such as well-known application stores. If organizations cannot enforce this policy through technical controls, they should provide security awareness training on the matter (see section 3.6).

Organizations with more mature IT infrastructure and business processes should 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.

For mobile connectivity, organizations should instruct users to disable automatic connections to open Wi-Fi networks and avoid unknown Wi-Fi networks. Organizations should consider using a VPN if they require connectivity to public Wi-Fi networks. Organizations should limit Bluetooth and other near-field communication (NFC) protocols for the exchange of sensitive information. Organizations should also instruct users to select the most secure connectivity option available, such as using data over cellular networks rather than public Wi-Fi networks.

To summarize:

BC.8.1 Organizations should decide on an ownership model for mobile devices and document the rationale and associated risks.

BC.8.2 Organizations should enforce separation between work and personal data on mobile devices with access to corporate IT resources and document the details of this separation.

BC.8.3 Organizations should ensure that employees only download mobile device apps from the organization's list of trusted sources.

BC.8.4 Organizations should require that all mobile devices store all sensitive information in a secure, encrypted state.

BC.8.5 Organizations should consider implementing 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.

BC.8.6 Organizations should enforce or educate users to: (1) disable automatic connections to open networks, (2) avoid connecting to unknown Wi-Fi networks, (3) limit the use of Bluetooth and NFC for the exchange of sensitive information, and (4) use corporate Wi-Fi or cellular data network connectivity rather than public Wi-Fi.

BC.8.7 Organizations should consider using a VPN if they require connectivity to public Wi-Fi networks OR provide the rationale for not using a VPN.

3.9 ESTABLISH BASIC PERIMETER DEFENCES

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. Organizations should implement dedicated firewalls at the boundaries between corporate networks and the Internet.

Organizations should install and configure a Domain Name System (DNS) firewall solution to prevent connections to known malicious web domains. Solutions are available to protect all devices connected to a corporate network. Organizations should also consider using a DNS firewall solution for content filtering to limit the websites accessible from the corporate network.

Organizations should require the use of secure connectivity to all of its online corporate IT services. If an organization permits employees to connect remotely into its networks from the Internet, they should set up a virtual private network (VPN) gateway and require that users access the organization's network via the VPN using two-factor authentication (see section 3.5). Additionally, a firewall must exist between the VPN termination point and the internal network.

Organizations operating an internal Wi-Fi network should use the WPA2 wireless security protocol or better. Where possible, organizations should use the strongest variant (e.g. WPA2-Enterprise) as it offers stronger individual user authentication. Organizations should consult their product documentation for how to configure these protocols. Furthermore, organizations should isolate the Wi-Fi network via a firewall that filters wireless network traffic entering the rest of its network.

Similarly, if an organization chooses to offer public Wi-Fi services for visitors and guests, the organization should never connect this public network to the organization's internal networks or resources such as printers or audiovisual systems.

Organizations should follow the Payment Card Industry Data Security Standard (PCI DSS) [11] for all Point-of-Sale (PoS) terminals and financial systems. Organizations should segment PoS terminals and financial systems, isolating them from the Internet and segmenting them from other areas of the corporate network via a firewall. Organizations should consider limiting PoS systems from having the ability to browse the Internet as well as internal services not related to their financial transaction and inventory control functions.

Organizations should filter spam or email with malicious attachments or links. To reduce the risks of fraudulent or deceptive email, organizations should ensure that their email service implements Domain-based Message Authentication, Reporting, and Conformance (DMARC) [12].

To summarize:

BC.9.1 Organizations should have dedicated firewalls at the boundaries between its corporate network and the Internet. The organization should isolate Internet-facing servers from the rest of their corporate network.

BC.9.2 Organizations should implement a DNS firewall for outbound DNS requests to the Internet.

BC.9.3 Organizations should require secure connectivity to all corporate IT resources and require VPN connectivity with two-factor authentication for all remote access into corporate networks.

BC.9.4 Organizations should only use secure Wi-Fi, preferably WPA2-Enterprise.

BC.9.5 Organizations should never connect public Wi-Fi networks to their corporate networks.

BC.9.6 Organizations should isolate point-of-sale systems from the Internet and other areas of the corporate network with a firewall. Organizations should consider following the Payment Card Industry Data Security Standard (PCI DSS).

BC.9.7 Organizations should ensure the implementation of DMARC on all of the organization's email services.

BC.9.8 Organizations should implement email filtering at points of ingress and egress.

3.10 SECURE CLOUD AND OUTSOURCED IT SERVICES

Organizations typically rely on outsourced IT service providers 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. Organizations should consider their comfort level with the regulations within the legal jurisdictions where their outsourced providers store or use their sensitive information.

Organizations should require that all their cloud service providers share an *AICPA SSAE 18 SOC 3* report [13] that states that they achieved Trust Service Principles compliance. If a provider cannot provide this certification, the organization should consider alternative providers.

Organizations should encrypt all sensitive information stored outside the premises of the organization, and ensure secure access to data stored in the cloud (e.g. using secure web browser connections).

Organizations should also consider all of the following regarding their cloud and outsourced IT providers:

- Privacy and data-handling policies;
- Notification processes when private data is accessed without prior authorization;
- Destruction processes for data at the end of the outsourcing contract;
- Physical location and security of outsourced data centres; and
- Physical location of outsourced administrators.

Further to section 3.5, organizations should require that all cloud-based administrative accounts implement two-factor authentication. Additionally, organizations should ensure that all cloud service accounts use different passwords (or other authentication factors) than those used within the organization's internal IT infrastructure.

To summarize:

BC.10.1 Organizations should require that all their cloud service providers share an *AICPA SSAE 18 SOC 3* report that states that they achieved Trust Service Principles compliance.

BC.10.2 Organizations should evaluate their comfort level with how their outsourced IT providers handle and access their sensitive information.

BC.10.3 Organizations should evaluate their comfort level with the legal jurisdictions where their outsourced providers store or use their sensitive information.

BC.10.4 Organizations should ensure that their IT infrastructure and users communicate securely with all cloud services and applications.

BC.10.5 Organizations should ensure that administrative accounts for cloud services use two-factor authentication and differ from internal administrator accounts.

3.11 SECURE WEBSITES

Organizations should ensure that the sensitive information handled by their websites is secure by following the Level 1 guidelines of *Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS)* [14]. Organizations should include meeting ASVS as a contractual requirement for outsourced websites, or be prepared to invest to meet these IT security requirements for websites developed and operated in-house.

To summarize:

BC.11.1 Organizations should ensure that their websites address the *OWASP top 10 vulnerabilities*.

BC.11.2 Organizations should ensure that they understand the ASVS level they need to meet for each of their websites.

3.12 IMPLEMENT ACCESS CONTROL AND AUTHORIZATION

Organizations should follow the principle of least privilege, where users have only the minimal functionality required to perform their tasks. Administrative accounts should face further restrictions – these accounts should permit only administrative actions and not user-level activities like browsing the web or accessing email. To ensure clear accountability for user activities, organizations should give all users unique individual accounts and minimize or eliminate the use of shared or shared-use accounts. Organizations should have a process in place to revoke accounts when they are no longer required, such as when employees leave the organization.

Larger organizations should implement centralized authorization control systems such as Lightweight Directory Access Protocol or Active Directory.

To summarize:

BC.12.1 Organizations should provision accounts with the minimum functionality necessary for tasks and, in particular, should restrict administrator privileges to an as-required basis.

BC.12.2 Organizations should only permit administrator accounts to perform administrative activities (and not user-level activities such as accessing email or browsing the web).

BC.12.3 Organizations should remove accounts and/or functionality when employees no longer require these for their tasks.

BC.12.4 Organizations should consider implementing a centralized authorization control system OR provide a rationale for not implementing a centralized authorization control system.

3.13 SECURE PORTABLE MEDIA

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. Since banning their use altogether may be impractical, we recommend that organizations limit the use of portable media to commercial encrypted drives provided by the organization.

We recommend maintaining strong asset control for all storage devices, including portable media devices. This control should include the proper disposal of such media. Organizations should ensure that they use the wipe functions provided by some devices (e.g. mobile devices and tablets) prior to disposal. For devices without such functionality, organizations should retain a service provider for their destruction.

To summarize:

BC.13.1 Organizations should mandate the sole use of organization-owned secure portable media, have strong asset controls for these devices, and require the use of encryption on all of these devices.

BC.13.2 Organizations should have processes for the sanitization or destruction of portable media prior to disposal.

4 SUMMARY

The baseline controls aim to advise and guide small and medium organizations on how to maximize the effectiveness of their cyber security investments. Organizations seeking to go beyond these controls should look to more comprehensive cyber security measures such as the *Center for Internet Security Controls* [15], the *NIST Cyber Security Framework* [5], *ISO/IEC 27001:2013* [6] or *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [4].

5 SUPPORTING CONTENT

5.1 LIST OF ABBREVIATIONS

Term	Definition
ASVS	Application Security Verification Standard
BYOD	Bring Your Own Device
CCCS	Canadian Centre for Cyber Security
CISO	Chief Information Security Officer
COPE	Company-Owned, Personally Enabled
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
EMM	Enterprise Mobility Management
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
NIST	US National Institute for Standards and Technology
OWASP	Open Web Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
PoS	Point-of-Sale
SD	Secure Digital
TLP	Traffic Light Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
Wi-Fi	Wireless local area networking
WPA2	Wi-Fi Protected Access II

5.2 GLOSSARY

Term	Definition
Authentication	A process or measure used to verify a user's identity.
Availability	The ability for the right people to access the right information or systems when required.
Commercial espionage	Spying directed toward the intellectual property or sensitive information of enterprises.
Confidentiality	The ability to protect sensitive information from access by unauthorized people.
Cybercrime	Crime that uses computers and computer networks.
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.
Encryption	Converting information from one form to another to hide its content and prevent unauthorized access.
Enterprise mobility management	Systems that manage mobile computing devices or services for an enterprise.

Term	Definition
Firewall	A security barrier placed between two networks 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.
Integrity	The ability to protect information from unauthorized modification or deletion.
Malware	Malicious software designed to infiltrate or damage a computer system, without the owner's consent.
Patching	The application of updates to computer software or firmware.
Ransomware	A type of malware that denies a user's access to a system or data until a sum of money is paid.
Residual Risk	The likelihood and impact of a threat that remains after security controls are implemented.
Sensitive information	Information that requires protection against unauthorized disclosure.
Two-factor authentication	A type of multi-factor authentication used to confirm the identity of a user. Authentication is validated by using a combination of two different authentication factors: something a user knows (e.g. a password), has (e.g. a physical token), or is (e.g. a biometric).

5.3 REFERENCES

Number	Reference
1	FIRST. *Traffic Light Protocol (TLP) Definitions and Usage*, available from https://www.first.org/tlp
2	Public Safety Canada. *National Cyber Security Strategy*, available from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
3	Canadian Centre for Cyber Security. *National Cyber Threat Assessment 2018*, available from https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018
4	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*, December 2014, available from https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33
5	NIST. *Cyber Security Framework*, available from https://www.nist.gov/cyberframework
6	ISO/IEC. *Information technology – Security techniques – Information security management systems – Requirements*, ISO/IEC 27001:2013, available from https://www.iso.org/standard/54534.html
7	Innovation, Science and Economic Development Canada. *SME Research and Statistics*, available from http://www.ic.gc.ca/eic/site/061.nsf/eng/Home
8	Gartner. *Gartner Says Many Organizations Falsely Equate IT Security Spending With Maturity*, December 2016, available from https://www.gartner.com/en/newsroom/press-releases/2016-12-09-gartner-says-many-organizations-falsely-equate-it-security-spending-with-maturity
9	Center for Internet Security. *Center for Internet Security Benchmarks*, available from https://www.cisecurity.org/cis-benchmarks
10	Canadian Centre for Cyber Security. *ITSP.30.31 V3 User Authentication Guidance for Information Technology Systems*, available from https://www.cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3
11	Payment Card Industry. *Payment Card Industry Data Security Standard (PCI DSS)*, available from https://www.pcisecuritystandards.org/security_standards/documents.php
12	Global Cyber Alliance. *Domain-based Message Authentication, Reporting and Conformance (DMARC)*, available from https://www.globalcyberalliance.org/dmarc
13	American Institute of Certified Public Accountants. *Statement on Standards for Attestation Engagement (SSAE) No. 18*, available from https://www.aicpa.org
14	Open Web Application Security Project. *Application Security Verification Standard*, available from https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf
15	Center for Internet Security. *Center for Internet Security Controls*, available from https://www.cisecurity.org/controls

Annex A Summary of the Baseline Controls

Number	Control
OC.1	Organizations using the baseline controls should have less than 499 employees.
OC.2	Organizations should list which parts of their information systems and assets are in scope for their implementation of the baseline controls and should provide the rationale for excluding information systems and assets and recognize the acceptance of risk in doing so.
OC.3	Organizations should assess the potential injury to the confidentiality, integrity, and availability to their information systems and assets.
OC.4	Organizations should self-identify their primary cyber threat.
OC.5.1	Organizations should identify someone in a leadership role who is specifically responsible for their IT security.
OC.5.2	Organizations should identify their financial spending levels for IT and IT security investment (as raw numbers and as a percent of total expenditures).
OC.5.3	Organizations should identify their internal staffing levels for IT and IT security (as raw numbers and as a percent of total staff).
OC.5.4	Organizations should commit to progressive improvements to cyber security.
BC.1.1	Organizations should have a basic 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.
BC.1.2	Organizations should have a written incident response plan that details who is responsible for handling incidents, including any relevant contact information for communicating to external parties, stakeholders, and regulators. Organizations should have an up-to-date hard copy version of this plan available for situations where soft copies are not available.
BC.1.3	Organizations should consider purchasing a cyber security insurance policy that includes coverage for incident response and recovery activities OR provide a rationale for not purchasing one.
BC.2.1	Organizations should enable automatic patching for all software and hardware OR establish full vulnerability and patch management solutions.
BC.2.2	Organizations should conduct risk assessment activities as to whether to replace any software and hardware that are not capable of automatic updates. If the organization chooses to keep such devices, they should have a business process to ensure regular manual updates.
BC.3.1	Organizations should enable anti-malware solutions that update and scan automatically.
BC.3.2	Organizations should activate any software firewalls included on the devices that are within organizational networks OR document the alternative measures in place instead of these firewalls.
BC.4.1	Organizations should implement secure configurations for all their devices, changing all default passwords, turning off unnecessary features, and enabling all relevant security features.
BC.5.1	Organizations should implement two-factor authentication wherever possible, and document all instances where they make the business decision not to do so. Organizations should require two-factor authentication for important accounts such as financial accounts, system administrators, cloud administration, privileged users, and senior executives.
BC.5.2	Organizations should enforce password changes on suspicion or evidence of compromise.
BC.5.3	Organizations should 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.
BC.6.1	Organizations should invest in cyber security awareness and training for their employees.
BC.7.1	Organizations should back up systems that contain essential business information and ensure that recovery mechanisms effectively and efficiently restore these systems from back-ups. Organizations should consider storing backups offline at a secure offsite location OR provide the rationale for not doing so.
BC.7.2	Organizations should securely store backups in an encrypted state and restrict access to them to those who must access them for the testing or use of restoration activities. Long term backups (e.g. weekly backups) must be stored offline, but frequent backups (e.g. daily backups) may be stored online.

Number	Control
BC.8.1	Organizations should decide on an ownership model for mobile devices and document the rationale and associated risks.
BC.8.2	Organizations should enforce separation between work and personal data on mobile devices with access to corporate IT resources and document the details of this separation.
BC.8.3	Organizations should ensure that employees only download mobile device apps from the organization's list of trusted sources.
BC.8.4	Organizations should require that all mobile devices store all sensitive information in a secure, encrypted state.
BC.8.5	Organizations should consider implementing 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.
BC.8.6	Organizations should enforce or educate users to: (1) disable automatic connections to open networks, (2) avoid connecting to unknown Wi-Fi networks, (3) limit the use of Bluetooth and NFC for the exchange of sensitive information, and (4) use corporate Wi-Fi or cellular data network connectivity rather than public Wi-Fi.
BC.8.7	Organizations should consider using a VPN if they require connectivity to public Wi-Fi networks OR provide the rationale for not using a VPN.
BC.9.1	Organizations should have dedicated firewalls at the boundaries between its corporate network and the Internet. The organization should isolate Internet-facing servers from the rest of their corporate network.
BC.9.2	Organizations should implement a DNS firewall for outbound DNS requests to the Internet.
BC.9.3	Organizations should require secure connectivity to all corporate IT resources and require VPN connectivity with two-factor authentication for all remote access into corporate networks.
BC.9.4	Organizations should only use secure Wi-Fi, preferably WPA2-Enterprise.
BC.9.5	Organizations should never connect public Wi-Fi networks to their corporate networks.
BC.9.6	Organizations should isolate point-of-sale systems from the Internet and other areas of the corporate network with a firewall. Organizations should consider following the Payment Card Industry Data Security Standard (PCI DSS).
BC.9.7	Organizations should ensure the implementation of DMARC on all of the organization's email services.
BC.9.8	Organizations should implement email filtering at points of ingress and egress.
BC.10.1	Organizations should require that all their cloud service providers share an *AICPA SSAE 18 SOC 3* report that states that they achieved Trust Service Principles compliance.
BC.10.2	Organizations should evaluate their comfort level with how their outsourced IT providers handle and access their sensitive information.
BC.10.3	Organizations should evaluate their comfort level with the legal jurisdictions where their outsourced providers store or use their sensitive information.
BC.10.4	Organizations should ensure that their IT infrastructure and users communicate securely with all cloud services and applications.
BC.10.5	Organizations should ensure that administrative accounts for cloud services use two-factor authentication and differ from internal administrator accounts.
BC.11.1	Organizations should ensure that their websites address the *OWASP top 10 vulnerabilities*.
BC.11.2	Organizations should ensure that they understand the ASVS level they need to meet for each of their websites.
BC.12.1	Organizations should provision accounts with the minimum functionality necessary for tasks and, in particular, should restrict administrator privileges to an as-required basis.
BC.12.2	Organizations should only permit administrator accounts to perform administrative activities (and not user-level activities such as accessing email or browsing the web).
BC.12.3	Organizations should remove accounts and/or functionality when employees no longer require these for their tasks.
BC.12.4	Organizations should consider implementing a centralized authorization control system OR provide a rationale for not implementing a centralized authorization control system.

Number	Control
BC.13.1	Organizations should mandate the sole use of organization-owned secure portable media, have strong asset controls for these devices, and require the use of encryption on all of these devices.
BC.13.2	Organizations should have processes for the sanitization or destruction of portable media prior to disposal.

Annex B Summary of Version Changes

Change	Description of change
1	In **OC.2**, the text "and should provide the rationale for excluding information systems and assets and recognize the acceptance of risk in doing so," was added.
2	In **OC.4**, the text "primary threat of concern" was changed to "primary cyber threat".
3	In **BC.7.1**, the text "storing backups at a secure offsite location" was changed to "storing backups offline at a secure offsite location".
4	In **BC.7.2**, the text "Long term backups (e.g. weekly backups) must be stored offline, but frequent backups (e.g. daily backups) may be stored online," was added.
5	**BC.9.8** is a newly added Baseline Control.
6	In **BC.11.1**, the text "Organizations should ensure that their websites meet the OWASP ASVS Level 1 guidelines" was changed to Organizations should ensure that their websites address the *OWASP top 10 vulnerabilities*".
7	**BC.11.2** is a newly added Baseline Control.