TOP MEASURES TO ENHANCE CYBER SECURITY FOR SMALL AND MEDIUM ORGANIZATIONS

CANADIAN CENTRE FOR CYBER SECURITY

JUNE 2021 | ITSAP.10.035

Looking for steps you can take to protect your organization's networks and information from cyber threats? To get you started, we have summarized the **13** security control categories that are identified in our *Baseline Cyber Security Controls for Small and Medium Organizations* and form the foundation for the **CyberSecure Canada Certification** program. By implementing these controls, you can reduce your risks and improve your ability to respond to security incidents. **While it isn't always necessary to implement all of the controls, we encourage you to adopt as many as possible to enhance your cyber security**.

DEVELOP AN INCIDENT RESPONSE PLAN

If you have a plan, you can quickly respond to incidents, restore critical systems and data, and keep service interruptions and data loss to a minimum. Your plan should include strategies for backing up data.

- *Developing Your IT Recovery Plan (ITSAP.40.004)*

USE STRONG USER AUTHENTICATION

Implement user authentication policies that balance security and usability. Ensure your devices authenticate users before they can gain access to your systems. Wherever possible, use two-factor authentication (2FA) or multi-factor authentication (MFA).

- *Secure Your Accounts and Devices With Multi-Factor Authentication (ITSAP.30.030)*
- *Best Practices for Passphrases and Passwords (ITSAP.30.032)*
- *Rethink Your Password Habits to Protect Your Accounts from Hackers (ITSAP.30.036)*

ENABLE SECURITY SOFTWARE

Activate firewalls and install anti-virus and anti-malware software on your devices to thwart malicious attacks and protect against malware. Ensure you download this software from a reputable provider. Install Domain Name System (DNS) filtering on your mobile devices to block out malicious websites and filter harmful content.

- *Preventative Security Tools (ITSAP.00.058)*

PATCH OPERATING SYSTEMS AND APPLICATIONS

When software issues or vulnerabilities are identified, vendors release patches to fix bugs, address known vulnerabilities, and improve usability or performance. Where possible, enable automatic patches and updates for all software and hardware to prevent threat actors from exploiting these issues or security vulnerabilities.

- *How Updates Secure Your Devices (ITSAP.10.096)*

BACK UP AND ENCRYPT DATA

Copy your information and critical applications to one or more secure locations, such as the cloud or an external hard drive. If a cyber incident or natural disaster happens, these copies can help you continue business activities and prevent data loss. Backups can be done online or offline and can also be done in three different iterations: full, differential or incremental. Test your backups regularly to ensure you can restore your data.

- *Tips for Backing Up Your Information (ITSAP.40.002)*

TRAIN YOUR EMPLOYEES

Tailor your training programs to address your organization's cyber security protocols, policies, and procedures. Having an informed workforce can reduce the likelihood of cyber incidents.

- *Offer Tailored Cyber Security Training to your Employees (ITSAP.10.093)*

HOW TO USE THESE CONTROLS

These controls are not a one-size-fits-all approach to cyber security. They are guiding principles that you can use to create your organization's own cyber security framework.

You should scope and tailor these controls based on your organization's needs and requirements. Implement as many of these controls as possible to enhance your cyber security posture and help minimize the risk of cyber attacks. Starting with the following four controls will strengthen your organization's security:

1. Develop an Incident Response Plan
2. Patch Operating Systems and Applications
3. Use Strong User Authentication
4. Backup and Encrypt Data

Before implementing the controls, keep the following tips in mind:

- Identify the critical information assets and systems to which you will apply these controls.
- Understand the main threats to your organization.
- Identify your valuable information and systems and apply risk management plans to enhance your security posture.
- Implement some or all of these controls and you will see a significant impact on improving your organization's resilience and protection against cyber threats.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

© Government of Canada | This document is the property of the Government of Canada. It shall not be altered, altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE. Cat. No. D97-1/10-035-2021E-PDF ISBN 978-0-660-39075-8

TOP MEASURES TO ENHANCE CYBER SECURITY FOR SMALL AND MEDIUM ORGANIZATIONS

CANADIAN CENTRE FOR CYBER SECURITY

OCTOBER 2020 |

SECURE CLOUD AND OUTSOURCED SERVICES

Get to know a service provider before you contract them. Make sure the service provider has measures in place to meet your security requirements and needs.

Know where a service provider's data centres are located. Different countries have different privacy laws and data protection requirements.

- *Benefits and Risks of Adopting Cloud-Based Services in Your Organization (ITSE.50.060)*
- *Models of Cloud Computing (ITSAP.50.111)*
- *Cyber Security Considerations for Consumers of Managed*

SECURE PORTABLE MEDIA

Storing and transferring data using a portable media device, like a USB key, is convenient and cost-effective, but they can be prone to loss or theft. Maintain an inventory of all assets.

Use encrypted portable storage devices, if possible, and sanitize devices properly before reusing or disposing of them.

- *Security Tips for Peripheral Devices (ITSAP.70.015)*
- *Sanitization and Disposal of Electronic Devices (ITSAP.40.006)*

CONFIGURE DEVICES SECURELY

Take the time to review your device's default settings and make modifications as required. At a minimum, we recommend changing default passwords (especially administrative passwords), turning off location services, and disabling unnecessary features.

- *Cyber Security at Home and in the Office: Secure Your Devices, Computers and Networks (ITSAP.00.007)*

SECURE MOBILE DEVICES

Choose a device deployment model. Will your organization provide employees with corporately owned devices or will you allow employees to use personal devices for work?

Ensure employees can only use approved applications and can only download applications from trusted sources.

- *Security Considerations for Mobile Device Deployments (ITSAP.70.002)*

SECURE WEBSITES

Protect your website and the sensitive information it collects. Encrypt sensitive data, ensure your certificates are up to date, use strong passwords or passphrases on the backend of the site, and use HTTPS for your site.

If you have outsourced your website, ensure your site's host has security measures in place.

- *Website Defacement (ITSAP.00.060)*

ESTABLISH BASIC PERIMETER DEFENCES

Defend your networks from cyber threats. For example, use a firewall to defend against outside intrusions by monitoring incoming and outgoing traffic and filtering out malicious sources.

Use a virtual private network (VPN) when employees are working remotely to secure the connection and protect sensitive information.

- *Virtual Private Networks (ITSAP.80.101)*

ACCESS CONTROL AND AUTHORIZATION

Apply the principle of least privilege to prevent unauthorized access and data breaches. Employees should only have access to the information that they need to do their jobs. Each user should have their own set of log-in credentials, and administrators should have separate administrative accounts and general user accounts.

- *Managing and Controlling Administrative Privileges (ITSAP.10.094)*

LEARN MORE

We've included a selection of our publications, but you can browse our entire catalogue at **cyber.gc.ca**.

These baseline cyber security controls are also the foundation of the **CyberSecure Canada Certification**. The certification program helps small and medium-sized organizations improve and demonstrate their cyber security. Implementing the certification requirements can help you protect your organization, clients, and partners from cyber attacks.

Why Get Certified?

- Improve your competitive advantage by reassuring your customers, partners, investors and suppliers that the valuable information they provide you will be secure.
- Limit the direct and indirect impacts on your business from cyber attacks: financial loss, damage to your reputation and critical infrastructure, litigation, job losses and increased consumer prices.
- Ensure your organization is eligible to compete for business opportunities that require cybersecurity certification.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

© Government of Canada | This document is the property of the Government of Canada. It shall not be altered, altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE. Cat. No. D97-1/10-035-2021E-PDF ISBN 978-0-660-39075-8