Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

TOP 10 IT SECURITY ACTIONS TO PROTECT INTERNET-CONNECTED NETWORKS AND INFORMATION

MANAGEMENT

Canada

FOREWORD

ITSM.10.089 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information is an unclassified publication issued under the authority of the Head of the Canadian Centre for Cyber Security.

This document supersedes *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* and *ITSB-89 v3 Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information*.

EFFECTIVE DATE

This publication takes effect on September 24, 2021.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	October 2018
2	Second released.	September 24, 2021

OVERVIEW

This document lists our top 10 mitigating actions that your organization should take to protect its Internet-connected networks and sensitive information from cyber security threats.

This version of the document includes considerations for consumers of cloud services and managed services. This document supersedes previous versions of *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* and *ITSB-89 v3 Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information*.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

This document lists our top 10 mitigating actions that your organization should take to protect its Internet-connected networks and sensitive information from cyber security threats. As you take each of these 10 actions, you add defensive layers to your environment, making it more difficult for threat actors to exploit vulnerabilities and compromise your networks, systems, and information.

While we recommend all 10 actions, we realize that your organization may not be able to take all of them. Your organization should conduct a risk assessment to determine its security requirements and priorities. When taking these actions, you should tailor them to your organization's environment and apply any additional security measures that are needed to protect your most sensitive systems and information.

For Government of Canada (GC) departments and agencies, see the cyber security requirements addressed in the GC *Directive on Service and Digital* [1][1]. If your organization is not part of the GC, you can refer to this policy when creating your own security program and policies. For more information on implementing baseline cyber security controls, see our *Baseline Cyber Security Controls for Small and Medium Organizations* [2].

[1] Numbers in square brackets indicate reference material cited in the Supporting Content section of this document.

2 THE TOP 10

Our top 10 includes prioritized security actions that your organization should take as a baseline to strengthen its IT infrastructure and protect its networks. Although we recommend following the numerical order of these actions (starting with #1) to increase your protection efforts against cyber threats, you can change the sequence of actions to meet your organization's needs and requirements. As you add security actions to your environment, your threat surface (i.e. all available endpoints that a threat actor may try to exploit) decreases, and your security posture increases.

Keep in mind that these actions are just a starting point, and there is no single strategy that is guaranteed to prevent cyber incidents. The cyber threat landscape continues to evolve, and you should ensure that you reassess your risks and review your current security efforts so that you can address any gaps or weaknesses.

When determining your security needs, you should also consider whether your organization is using cloud or managed services. You should assess the threats, vulnerabilities, shared responsibilities, and cloud platform capabilities so that you can implement the appropriate security controls. The ways in which you follow the top 10 security actions may differ depending on the types of services you are using. For example, the roles and responsibilities of your organization and the cloud service provider (CSP) or managed service provider (MSP) will vary depending on the services you are consuming and your service model and deployment model. However, even when using cloud or managed services, your organization is still legally responsible and accountable for securing its data. For more information on security and cloud or managed services, see *ITSM.50.062 Cloud Security Risk Management* [3] and *ITSM.50.030 Cyber Security Considerations for Consumers of Managed Services* [4].

Figure 1: Top 10 IT Security Actions

2.1 CONSOLIDATE, MONITOR, AND DEFEND INTERNET GATEWAYS

Action #1 is to consolidate, monitor, and defend your Internet gateways. Your Internet gateways are checkpoints that are installed at the edge of your network. Gateways monitor all incoming and outgoing traffic to protect your organization. GC departments and agencies should reduce the number of discrete external connections to their departmental networks by using Shared Services Canada's consolidated Internet gateways.

Your organization should also monitor its Domain Name System (DNS) server. The Canadian Internet Registration Authority (CIRA) offers a free protected DNS service, Canadian Shield, that prevents you from connecting to malicious websites that might infect devices or steal personal information.

Your organization is responsible for monitoring all incoming and outgoing traffic at these gateways, even if you are using cloud services. To simplify this task, reduce the number of external connections to your network. You should establish a baseline of normal traffic patterns first, which enables you to detect and react to changes in these patterns.

When using cloud services, you should also consider the flow of data from your organization to any cloud systems or services. Depending on the sensitivity of the data that is being transmitted to these services and the Transport Layer Security (TLS) version that the provider is using, you may want to use a virtual private network (VPN). A VPN creates a secure connection between two points and can be used to protect sensitive data while it is in transit between those points. Depending on the sensitivity of your data, you may want to consider procuring dedicated connection patterns (i.e. how your organization connects to the cloud services). In this case, you will need to negotiate with your provider, and you may need to configure and implement measures such as Internet Protocol Security (IPsec) or Media Access Control Security (MACsec).

You may also outsource monitoring activities to a managed security service provider (MSSP). If you are working with a service provider that offers secure gateway services, you should clearly identify the roles and responsibilities that your organization and the service provider have for monitoring traffic and reporting anomalies or malicious activities.

You can implement additional cyber defences that monitor for and respond to unauthorized entry, data exfiltration, or other malicious activities. If malicious activity is detected, these cyber defences should be able to shut down access points to stop data exfiltration or block unwanted attacks.

Related Publications:

- *ITSM.50.030 Cyber Security Considerations for Consumers of Managed Services* [4]
- *ITSAP.80.101 Virtual Private Networks* [5]

2.2 PATCH OPERATING SYSTEMS AND APPLICATIONS

Action #2 is to patch your organization's operating systems and applications regularly. Updates and patches do not just fix bugs or improve usability or performance; they address known security vulnerabilities.

Implement a patch management policy for operating systems and third-party applications to reduce your organization's exposure to publicly known vulnerabilities. When a vendor issues a security patch, you should follow your patch management process to apply the patch as soon as possible. You can use an automatic patch management system to apply patches in a timely manner.

Use supported, up-to-date, and tested versions of operating systems and applications. Using unsupported operating systems or applications, for which updates are not provided, increases your risk of exposure to exploitation because there is no mechanism available to mitigate vulnerabilities.

If you have outsourced your IT services to a CSP or an MSP, you should review your service contract to identify the roles and responsibilities related to patch management; the roles and responsibilities will vary depending on your cloud service model. For example, in the case of an infrastructure as a service (IaaS) or a platform as a service (PaaS) model, you are responsible for updating and patching your systems and applications. In a software as a service (SaaS) model, the CSP is responsible for updating and patching. However, even if you are using a service provider, you are still responsible for updating and patching peripheral devices and any systems and devices that fall out of the scope of the contract.

Related Publications:

- *ITSAP.10.096 How Updates Secure Your Device* [6]

2.3 ENFORCE THE MANAGEMENT OF ADMINISTRATIVE PRIVILEGES

Action #3 is to enforce the management of administrative privileges. Apply the principle of least privilege to ensure that users only have the access and the privileges they need to carry out their job functions. You should limit the number of administrative or privileged users for operating systems and applications.

Create different levels of administrative accounts so that, if an administrative account is compromised, the level of exposure is limited. To prevent exposure from phishing attacks or malware, administrators should perform administrative functions on dedicated workstations that do not have Internet or open email access, or that have Internet and email disabled from administrative accounts. Administrators should have separate administrative accounts and general user accounts; administrators should use their administrator accounts only for administrative tasks and use their general user accounts for other tasks (e.g. checking emails). If the same host is used to conduct administrative and general user activities, there is a risk that the host will be compromised when carrying out general activities (e.g. opening or interacting with a malicious email, clicking on malicious links). If the host if compromised, the user's administrative credentials may also be compromised. Generally, a compromised user account is easier to respond to than a compromised administrative account.

Your organization should implement an administrative password solution to protect passwords. To improve the assurance of user credentials, we highly recommend that you use multi-factor authentication (MFA), wherever possible, for all users and applications.

Frequently review and revalidate your organization's list of administrative users; you should ensure that privileges are revoked when users no longer require them (e.g. personnel and role changes).

If you are using cloud services, you are still responsible for managing access control. If you have outsourced your IT services to an MSP, you should be aware of who needs to be a privileged user.

Related Publications:

- *ITSAP.10.094 Managing and Controlling Administrative Privileges* [7]
- *ITSAP.30.030 Secure Your Accounts and Devices with Multi-Factor Authentication* [8]

2.4 HARDEN OPERATING SYSTEMS AND APPLICATIONS

Action #4 is to harden your organization's operating systems and applications. Your organization should be aware of all the applications that are used. Default configurations and misconfigurations can leave your networks, systems, and devices vulnerable. You should apply additional security controls to harden operating systems. For more information on selecting and applying security controls, see *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [9].

To prevent compromises of Internet-connected assets and infrastructures, your organization should disable all non-essential ports and services and remove all unnecessary accounts. Assess all third-party applications for components or functions that are not needed and should be disabled or require human intervention before they are enabled (i.e. macros). You should also have enterprise-level auditing and an anti-malware solution as part of your secure configuration.

If using cloud or managed services, your provider may be responsible for hardening operating systems and applications, depending on your service and deployment models. For example, in an IaaS or a PaaS model, your organization is responsible for hardening operating systems and applications; in a SaaS model, the service provider is responsible for hardening operating systems and applications. Your organization is responsible for all its on-premises equipment when incorporating any hybrid components or solutions.

Related Publications:

- *ITSP.70.012 Guidance for Hardening Microsoft Windows 10 Enterprise* [10]

2.5 SEGMENT AND SEPARATE INFORMATION

Action #5 is to segment and separate information. Your organization should have an inventory of its essential business information that is classified and categorized based on its level of sensitivity or impact on privacy.

Your networks should be zoned by segmenting and grouping infrastructure services that have the same information protection requirements or that must adhere to the same communication security policies. This logical design approach controls and restricts access and data communication flows. You should also continuously monitor and enforce controls to maintain zone protection and integrity.

The principles of zoning still apply if your organization is using cloud or managed services. If using a shared cloud deployment model, for example, you should ensure that your data is separated from other tenants' data.

Related Publications:

- *ITSP.80.022 Baseline Security Requirements for Network Security Zones* [11]
- *ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones* [12]

2.6 PROVIDE TAILORED TRAINING

Action #6 is to provide your employees with tailored cyber security training. Although system safeguards are expected to prevent malicious activity on networks, there are many factors to consider when managing risks. You can lower your organization's level of risk by training employees on cyber security issues and their roles and responsibilities in protecting networks, systems, and IT assets.

Your organization should initiate awareness and training activities to address cyber threats, vulnerabilities, and policy requirements (e.g. expected user behaviours). You should frequently review your IT security awareness programs and activities, and you should also ensure that they are accessible to all users who have access to organizational systems.

Our website (**cyber.gc.ca**) has a catalogue of publications on various cyber security topics. You can use these publications to increase employee awareness of cyber threats and best practices. You can also refer to Get Cyber Safe, which is a national public awareness campaign created to inform Canadians about cyber security.

Related Publications:

- *ITSM.10.093 Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training* [13]
- *ITSAP.10.093 Offer Tailored Cyber Security Training to Your Employees* [14]

2.7 PROTECT INFORMATION AT THE ENTERPRISE LEVEL

Action #7 is to protect information at the enterprise level. Your organization's information is valuable to your continued operation, but it is also a valuable target to threat actors. You should ensure that you are managing information appropriately through its lifecycle (e.g. data labelling, handling, retention, and destruction).

When deploying mobile devices in your organization, you should consider the risks and benefits of various deployment models. If it makes business sense, your organization should provide equipment (e.g. servers, desktops, laptops, mobile devices) to employees, using a device management framework and a configuration change management process. If your organization chooses to allow employees to use their personal devices for business, you should implement a strict control policy and review technologies and legal requirements for segregating business and personal information. Your organization can use unified endpoint management (UEM) to maintain the security of mobile devices. UEM combines features from mobile device management and enterprise mobility management processes.

You may use systems and services provided by CSPs, MSPs, or MSSPs. Regardless, your organization is always legally responsible and accountable for protecting its data. When data is stored outside of your organization's infrastructure, you need to know where it is stored (i.e. the geographical location). Data stored outside of Canada is subject to different privacy, security, and data ownership laws and regulations. If you are using cloud or managed services that store data outside of Canada, review the applicable laws of the geographic location where the data will reside and the possible impacts to privacy.

Note: GC departments and agencies are responsible for ensuring their computing facilities located within the geographic boundaries of Canada or within the premises of a GC department located abroad (e.g. Canadian consulate) are identified and evaluated as a principal delivery option for all sensitive electronic information and data (i.e. Protected B, Protected C, and Classified) under GC control. Preferably, GC departments and agencies should keep sensitive information within Canada; however, departments are responsible for conducting their risk assessments, based on the nature and the sensitivity of the data, and identifying their availability requirements. See the *Directive on Service and Digital* [1] for more information.

Related Publications:

- *ITSAP.10.016 Security Tips for Organizations with Remote Workers* [15]
- *ITSAP.70.002 Security Considerations for Mobile Device Deployments* [16]

- *ITSAP.50.112 Steps to Address Data Spillage in the Cloud* [17]

2.8 APPLY PROTECTION AT THE HOST LEVEL

Action #8 is to apply protection at the host level. You should deploy a host-based intrusion prevention system (HIPS) to protect your organization's systems against both known and unknown malicious attacks, such as viruses and malware. There are many commercial vendors that provide HIPS services.

HIPS take active measures to protect computer systems against intrusion attempts by using pre-defined sets of rules to recognize suspicious behaviour. When this behaviour is identified, the HIPS mechanism blocks the offending program or process from carrying out potentially harmful activity. You should continue to monitor HIPS alerts and logging information to identify indications of intrusions.

When using cloud services, you still need to apply protection at the host level and should consider cloud endpoints, data transmission, and your tenancy (e.g. edge and perimeter). We recommend that you use the specific tool sets provided by your selected CSP and any possible third-party tools that you could also apply.

2.9 ISOLATE WEB-FACING APPLICATIONS

Action #9 is to isolate all web-facing applications. Your organization should use virtualization to create an environment where web-facing applications can run in isolation (i.e. in a sandbox). By isolating these applications, malware, for example, is confined to your virtualized environment and cannot spread and infect the host or enterprise.

Related Publications:

- *ITSAP.70.011 Virtualizing Your Infrastructure* [18]

2.10 IMPLEMENT APPLICATION ALLOW LISTS

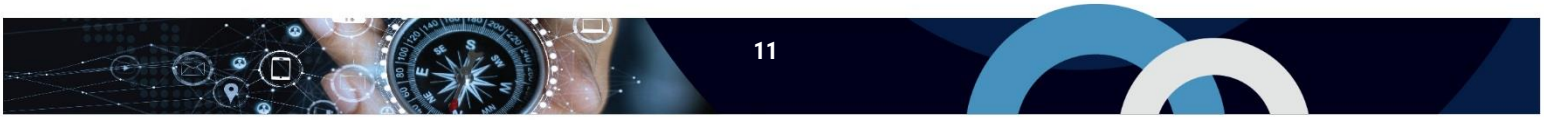
Action #10 is to implement application allow lists. An allow list specifies applications and application components (e.g. executable programs, software libraries, configuration files) approved to run on organizational systems. By implementing application allow lists, you can prevent malicious applications from being downloaded and infecting your servers and systems.

Your organization should create this list of applications that are authorized for use in the workplace and that are known to be from trustworthy vendors. All other applications and application components should be denied by default. You can define your allow list by using file and folder attributes (e.g. file path, file name, file size, digital signature or publisher, or cryptographic hash). You should define and deploy policies on allow lists across the organization. Remember to update your allow list when you patch or install an update for an application or when you start or stop using software.

If working with a CSP or MSP to set up your application allow lists, you should consider the sensitivity of your data and define and control your data access policies. Implement additional data security controls to restrict access to your data, according to your data sensitivity policies.

Related Publications:

- *ITSB-95 Application Allow Lists Explained* [19]



3 SUMMARY

This document lists our top 10 IT security actions, which your organization can apply as a baseline of security measures. By taking all these measures, you can reduce your organization's threat surface and improve your security posture. However, these actions are just a starting point. Your organization should continue to assess its threats and risk to ensure that you implement security controls that meet your security needs. If you are using cloud or managed services, you should consider the additional threats and risks and identify the roles and responsibilities related to these security actions.

3.1 CONTACT INFORMATION

If you would like more information on how to implement the top 10 IT security actions, visit us at cyber.gc.ca or contact our Contact Centre.

Cyber Centre Contact Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

4 SUPPORTING CONTENT

4.1 LIST OF ABBREVIATIONS

Term	Definition
CSP	Cloud service provider
GC	Government of Canada
HIPS	Host-based intrusion prevention system
IaaS	Infrastructure as a service
IPsec	Internet protocol security
IT	Information technology
MACsec	Media access control security
MFA	Multi-factor authentication
MSP	Managed service provider
MSSP	Managed security service provider
PaaS	Platform as a service
SaaS	Software as a service
TBS	Treasury Board of Canada Secretariat
TLS	Transport Layer Security
UEM	Unified endpoint management
VPN	Virtual private network

4.2 GLOSSARY

Term	Definition
Application allow list	A control list that identifies which applications are approved to execute and run on an organization's systems.
Cloud deployment model	Deployment models describe the relationship between the cloud service provider and the consumer. There are four cloud deployment models, including public, private, community, and hybrid.
Cloud service model	A service model describes the type of service that is provided to consumers. There are three different cloud service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
Cloud service provider	Any commercial provider that offers cloud computing services to provide on-demand availability of computer system resources.
Data in transit	Data that is active and moving from one location to another, such as across the Internet or within a private network.
Host-based intrusion prevention system	Software that monitors a single host for suspicious activity. HIPS take active measures to protect computer systems against intrusion attempts by using pre-defined sets of rules to recognize suspicious behaviour.
Least privilege	The security principle of giving an individual only the set of privileges that are essential to performing authorized tasks.
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, adware, and ransomware.
Managed security service provider	A service provider that monitors and manages security devices and systems on behalf of a customer.
Managed service provider	A company that remotely manages IT infrastructure and user end systems on behalf of a customer.
Multi-factor authentication	An authentication method in which two or more authentication factors (e.g. something you know, something you are, something you have) are required to confirm the identity of a user.
Network security zone	A networking environment with a well-defined boundary, a network security zone authority, and a standard level of weakness to network threats. Types of zones are distinguished by security requirements for interfaces, traffic control, data protection, host configuration control, and network configuration control.
Risk	The likelihood and the impact of a threat actor exploiting a vulnerability to access an asset. Expressed in degrees (e.g. high, medium, low).
Transport Layer Security	An authentication and security protocol used to provide privacy and data integrity between two communications applications [20].
Unified endpoint management	A software tool used to distribute, manage, and control endpoint devices (e.g. desktop and mobile devices).
Virtualization	The simulation of the software or hardware upon which other software runs [20].
Virtual private network	A private communications network usually used within a company, or by several different companies or organizations to communicate over a wider network. VPN communications are typically encrypted or encoded to protect the traffic from other users on the public network carrying the VPN.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization's assets or operations.

4.3 REFERENCES

Number	Reference
1	Treasury Board of Canada Secretariat. *Directive on Service and Digital*. 1 April 2020.
2	Canadian Centre for Cyber Security. *Baseline Security Controls for Small and Medium Organizations*. February 2020.
3	Canadian Centre for Cyber Security. *ITSM.50.062 Cloud Security Risk Management*. March 2019.
4	Canadian Centre for Cyber Security. *ITSM.50.030 Cyber Security Considerations for Consumers of Managed Services*. October 2020.
5	Canadian Centre for Cyber Security. ITSAP.80.101 Virtual Private Networks. October 2019.
6	Canadian Centre for Cyber Security. *ITSAP.10.096 How Updates Secure Your Devices*. February 2020.
7	Canadian Centre for Cyber Security. *ITSAP.10.094 Managing and Controlling Administrative Privileges*. July 2020.
8	Canadian Centre for Cyber Security. *ITSAP.30.030 Secure Your Accounts and Devices with Multi-Factor Authentication*. June 2020.
9	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
10	Canadian Centre for Cyber Security. *ITSP.70.012 Guidance for Hardening Microsoft Windows 10 Enterprise*. March 2019.
11	Canadian Centre for Cyber Security. *ITSP.80.022 Baseline Security Requirements for Network Security Zones*. February 2021.
12	Canadian Centre for Cyber Security. *ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones*. May 2009.
13	Canadian Centre for Cyber Security. *ITSM.10.093 Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training*. February 2020.
14	Canadian Centre for Cyber Security. *ITSAP.10.093 Offer Tailored Cyber Security Training to Your Employees*. October 2020.
15	Canadian Centre for Cyber Security. *ITSAP.10.016 Security Tips for Organizations with Remote Workers*. May 2020.
16	Canadian Centre for Cyber Security. *ITSAP.70.002 Security Considerations for Mobile Device Deployments*. June 2020.
17	Canadian Centre for Cyber Security. *ITSAP.50.112 Steps to Address Data Spillage in the Cloud*. September 2019.
18	Canadian Centre for Cyber Security. *ITSAP.70.011 Virtualizing Your Infrastructure*. September 2020.
19	Canadian Centre for Cyber Security. *ITSB-95 Application Allow Lists Explained – IT Security Bulletin for the Government of Canada.* March 2015.
20	National Institute for Standards and Technology. *Computer Security Resource Centre Glossary*. N.D.