Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

GUIDANCE FOR HARDENING MICROSOFT WINDOWS 10 ENTERPRISE

ITSP.70.012

March 2019

PRACTITIONER SERIES

Canada

FOREWORD

ITSP.70.012 Guidance for Hardening Microsoft Windows 10 Enterprise is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded to the Canadian Centre for Cyber Security's Contact Centre.

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

EFFECTIVE DATE

This publication takes effect on March 1, 2019.

OVERVIEW

This document provides technical guidance on Microsoft security features and tools that can be used to harden Windows 10 Enterprise Edition operating systems ("Windows 10"). Some recognized workarounds and fixes for known security issues in Windows 10 are included. This document introduces the baseline configurations for group policy object (GPO) settings, which are detailed in a separate document. The instructions on how to get a copy of the *Government of Canada (GC) Security Baseline Configurations for Windows 10* [1][1] are in section 8.1 of this document.

Windows 10 is a commonly used desktop operating system. While this document was written primarily for GC departments, non-GC organizations may also apply these recommendations.

At the time of this document's publication, the security features and tools listed in this document are Microsoft's most recent service offerings for Windows 10 (release 1607). This document may be updated to ensure all relevant security features and tools are captured. The GPO settings will also be updated to reflect Microsoft's bi-annual releases.

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

To prevent compromises to IT systems and networks, one of our recommended top 10 security actions is to harden operating systems (for more details, see *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* [2]).

This document includes Microsoft security features and tools that can be used to harden Windows 10 Enterprise Edition operating systems ("Windows 10"). Some workarounds and fixes for known security issues in Windows 10 (release 1607) are also included. Although this document was written primarily for GC departments, non-GC organizations may also apply these recommendations. These recommendations apply only to Windows 10 endpoint devices and not to Windows Server.

This document introduces two baseline configurations for group policy object (GPO) settings: minimum baseline settings and enhanced baseline settings. The minimum baseline settings are required for GC departments. These minimum baseline settings provide most endpoint devices with the required level of mitigation against security threats. If systems and networks hold Protected B information, the enhanced baseline settings and additional security measures must be implemented. However, the additional security measures are not within the scope of this document.

This document only introduces the baseline configurations. You must refer to the *GC Security Baseline for Windows 10* [1] for more detail. See the instructions on how to get a copy of the *GC Security Baseline for Windows 10* [1] in section 8.1 of this document.

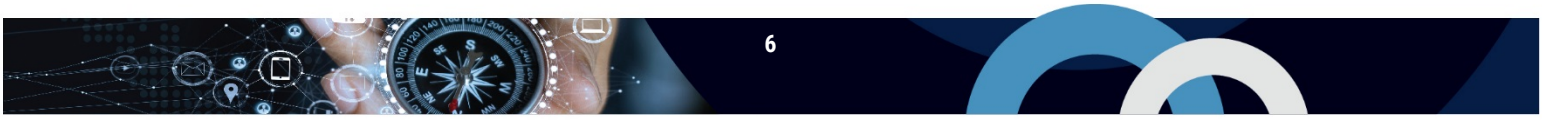
We worked with Shared Services Canada (SSC) to design GPO settings to minimize the risk of a threat actor compromising GC IT assets within common desktop operating environments and Internet-facing systems and networks. Compromises to systems and networks can be costly and threaten the availability, confidentiality, and integrity of information assets. GC departments are required to implement the baseline settings to standardize desktops. Standardized desktops provide security economies of scale and minimize custom patch management challenges.

1.1 POLICY DRIVERS

GC departments must comply with the policy requirements established in the following Treasury Board of Canada Secretariat (TBS) policies:

- Policy on Management of Information Technology [3]
- Policy on Government Security [4]
- Operational Security Standard: Management of Information Technology Security [5]
- IT Policy Implementation Notice (ITPIN). Direction on Windows 10 Desktop Operating System Migration and Configuration [6]

Non-GC organizations may refer to these policies when developing their policy frameworks.



1.2 APPLICABLE ENVIRONMENTS

This document provides guidance only for unclassified IT systems that may hold partially sensitive information (i.e. personal information[2] and business information[3]) or assets. Within the GC context, this guidance can be applied to IT systems that hold Protected A and/or Protected B information.

This document does not provide guidance for IT systems that hold **highly sensitive information or assets of individual interest** (i.e. Protected C information within the GC context) and **sensitive information or assets of national interest** (i.e. classified information[4]). IT systems that hold this type of information require additional design considerations that are not within the scope of this document.[5]

1.3 RELATIONSHIP TO THE IT RISK MANAGEMENT PROCESS

Departments should consider the baseline settings outlined in this publication when planning and implementing Windows 10. Departments are responsible for determining their requirements and risk management frameworks to help them protect information and services appropriately. *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [7] outlines two levels of IT security risk management activities: departmental-level activities and information system-level activities. Figure 1 on the next page provides an overview of these activities.

1.3.1 DEPARTMENTAL-LEVEL ACTIVITIES

Departmental-level activities are integrated into the departmental security program to plan, manage, assess, and improve the management of IT security-related risks. Annex 1 of ITSG-33 [7] describes these activities in more detail.

1.3.2 INFORMATION SYSTEM-LEVEL ACTIVITIES

Information system-level activities are integrated into the information system lifecycle. These activities ensure the following objectives are met:

- IT security needs of supported business activities are met
- Appropriate security controls are implemented and operate as intended
- Performance assessments of implemented security controls are conducted and the results are reported to ensure issues are addressed

[2] As defined in the Privacy Act and the Personal Information Protection and Electronic Documents Act, personal information is "information about an identifiable individual that is recorded in any form".

[3] Business information in this context refers to information that may reasonably be expected to cause injury to an organization, as defined in subsection 20(1) of the Access to Information Act.

[4] Within the GC context, classified information is any information or assets that, if compromised, could reasonably be expected to cause injury to the national interest, defense, and maintenance of the social, political, and economic stability of Canada. Information is classified at the Confidential, Secret, and Top Secret levels, depending on the type of information and the potential injury.

[5] Contact the CCCS Contact Centre for guidance regarding cryptographic solutions in PROTECTED C or Classified environments.

Annex 2 of ITSG-33 [7] describes the IT security risk management activities for implementing, operating, and maintaining dependable information systems through their lifecycle. Annex 2 also suggests a Secure Systems Development Lifecycle (SSDLC) process, referred to as the Information System Security Implementation Process (ISSIP).

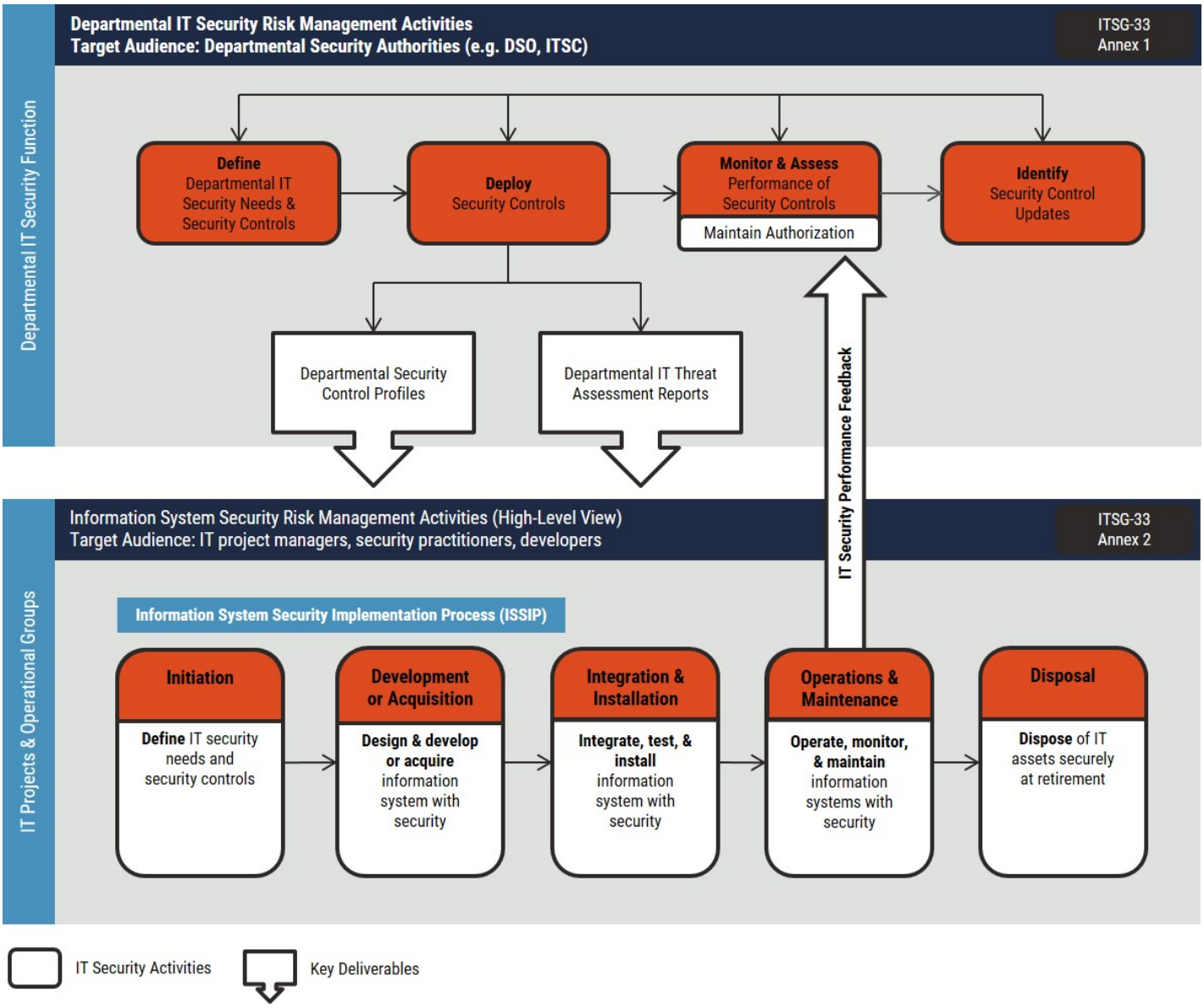


Figure 1: IT Security Risk Management Activities

2 CONSIDERATIONS

Before reconfiguring or upgrading IT systems or their components, organizations should consider their specific business needs and security requirements by taking the following actions:

- Identifying all enterprise architecture design and security requirements
- Completing a threat and risk assessment (TRA)
- Identifying hardware and firmware components for endpoint devices

2.1 ENTERPRISE ARCHITECTURE DESIGN AND SECURITY REQUIREMENTS

All enterprise architecture design and security requirements should be identified before applying the recommendations in this document. A full picture of the complete enterprise architecture will help departments identify the appropriate security features and tools for their business needs and security requirements. Once security features and tools are implemented, departments should continue to monitor these features and tools as a part of ongoing risk management activities. Regular monitoring ensures security controls continue to be effective.

2.2 THREAT AND RISK ASSESSMENTS

Departments should conduct TRAs as part of their ongoing risk management activities. A TRA should identify business, operational, and security needs. A TRA should also indicate the department's current security posture and include all planned or existing security controls. Departments can use the results of their TRAs to identify the Windows 10 configuration that best suits their needs. If an immediate upgrade or reconfiguration of Windows 10 is not possible, departments should identify and implement interim security risk management strategies and actions based on the results of their TRAs.

2.3 HARDWARE AND FIRMWARE

Departments should consider hardware and firmware when buying and implementing endpoint devices (e.g. servers, desktops, laptops, tablets). New endpoint devices should be set up with the hardware and firmware components identified in Microsoft's *Device Security* [8] guidelines.[6] To leverage new security functionality within Windows 10, the following hardware and firmware components should be in place:

- Unified extensible firmware interface (UEFI) (not configured to run in legacy basic input and output system [BIOS] mode) to enable Secure Boot. UEFI must support secure firmware updates
- Trusted platform module (TPM) 2.0. Some devices that use TPM 1.2 can be upgraded
- Hard drive formatting with global unique identifier (GUID) partition table (not master boot record [MBR] formatting)
- Hypervisor code integrity (HVCI) to ensure Device Guard can be implemented
- 64-bit CPU with Intel virtualization technology (VT-x) or Advanced Micro Dynamics virtualization (AMD-V) and extended page tables. Also called second level address translation (SLAT)

[6] Microsoft's *Device Security* guidelines are becoming an industry standard.

3 MITIGATION STRATEGY

To prevent compromises to Internet-connected assets and infrastructures, we have outlined 10 recommended security actions in ITSM.10.189 *Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* [2]. One of these security actions is to harden operating systems by disabling non-essential ports and services, removing unnecessary accounts, assessing third-party applications, and applying further security controls. When considering how to harden operating systems, the use of the default, out-of-the-box configuration of Windows 10 does not provide an adequate level of security for GC IT systems, networks, and information assets. We recommend configuring Windows 10 with the security features listed in section 4.1 of this document.

With regard to the GPO settings, departments are required to implement the minimum baseline settings outlined in section 5 of this document. The minimum baseline settings are the standard for GC departments because they provide most endpoint devices with the required level of mitigation against security threats. Departments with systems that may hold sensitive information or assets that, if compromised, could reasonably be expected to cause injury to the individual interest (e.g. a person or an organization) require additional levels of security. Within the GC context, this category of information is designated as Protected B information. Departments with systems operating in Protected B environments are required to implement the enhanced baseline settings, along with additional measures that are not covered in this document, to help protect sensitive information.

> **Note:** Based on the results of the TRA, departments may find that additional security-related functionality is required for Protected B operations.

To harden operating systems, we recommend that all departments implement both the minimum and enhanced baseline settings. These settings should be implemented with additional security measures to address department-specific needs.

4 WINDOWS 10 CONFIGURATION

Hardening operating systems is one of our top 10 recommended IT security actions. Operating systems can be hardened by configuring them with additional security features. This section outlines the Windows 10 security features and tools that we recommend implementing. Your Windows 10 configurations should align with the requirements outlined in TBS' *Direction on Windows 10 Desktop Operating System Management and Configuration* [6].

4.1 RECOMMENDED WINDOWS 10 SECURITY FEATURES AND TOOLS

Windows 10 should be configured with the security features and enhancements listed in Table 1. All the recommended security features and enhancements are either available in Windows 10 (release 1607) or can be downloaded for free from Microsoft.

Table 1: Recommended Windows 10 Security Features and Enhancements

Feature	Description
BitLocker	A full-disk encryption feature validated by the Cryptographic Module Validation Program (CMVP). This feature provides the capability to protect data at rest in the Windows 10 environment from offline attacks or malicious boots from another operating system. To encrypt GC data, BitLocker must be configured in Federal Information Processing Standards (FIPS) mode. **Note**: We do not recommend using CMVP modules outside of FIPS mode when encrypting GC information.
Enhanced Mitigation Experience Toolkit (EMET)	A feature to prevent the exploitation of software vulnerabilities found on legacy and third-party applications. The mitigation techniques employed by EMET include data execution prevention, structured exception handler overwrite protection, and anti-return-oriented programming. **Note**: EMET has been deprecated and will not be supported on *Windows 10 Fall Creators Update (1709)* [9]. EMET's capabilities have been rolled into the Exploit Protection feature of Windows Defender Exploit Guard.
AppLocker	An extension of the earlier Microsoft Software Restriction Policy feature. This feature provides flexible definition options for application whitelisting. Application whitelisting technologies control which applications are permitted to be installed or executed on a host. Whitelisting is a recommended top 10 security action in ITSM.10.189 [2]. For more information, see *ITSB-95 Application Whitelisting Explained* [10].
Secure Boot	A security standard feature used to ensure that endpoints boot using software trusted by the PC manufacturer. Each piece of software is validated against a database of known good signatures that are maintained in the firmware.
Device Guard	A set of hardware and security features that uses virtualization-based security to ensure that the operating system runs only trusted applications as defined in the department's code integrity policies.

Feature	Description
Credential Guard	A Windows 10 feature that protects systems from credential-theft attacks. The Credential Guard feature uses virtualization-based security to isolate secrets (e.g. new technology local area network manager [NTLM] password hashes and Kerberos ticket granting tickets) from the rest of the operating system.
Microsoft Desired Configuration Manager (DCM)	A feature from Microsoft's Security Compliance Manager (SCM) that can be used to assess the compliance of a Windows host against a desired baseline. Compliance verification can include the operating system version, application configuration, updates, and other security settings. **Note**: This feature is now called Compliance Settings in *System Center Configuration Manager Current Branch* [11]. The compliance settings provide the following capabilities: • Compare the configuration of Windows PCs, Mac computers, servers, and mobile devices and manage against best practice configurations that have been created or obtained from other vendors • Identify unauthorized device configurations • Report compliance with regulatory policies and in-house security policies • Identify security vulnerabilities • Provide the help desk with information to detect probable causes of reported incidents and problems by identifying non-compliant configurations • Remediate automatically some non-compliant settings on mobile devices The compliance settings also allow for the identification and remediation of "non-compliance" vulnerabilities by logging the "non-compliance" of applications, packages and programs, or scripts to a common file store. The common file store is routinely populated with devices reported to be "out of compliance".
Microsoft Office Isolated Conversion Environment (MOICE)	A feature added to the Microsoft Office Compatibility Pack to more securely open Word, Excel, and PowerPoint binary files included as email attachments. **Note**: MOICE is a capability in Office 2007 that has been rolled into Protected View[7] in Office 2010 and later versions.

[7] "Protected View is a new security feature in Office 2013 that evolved from the Microsoft Office Isolated Converter Environment (MOICE) in Office 2007. Protected View helps mitigate exploits to your computer by opening files in a restricted environment so they can be examined before they are opened for editing in Microsoft Excel 2013, PowerPoint 2013, or Word 2013. Protected View opens potentially dangerous files in a sandbox environment." Microsoft. *What is Protected View?* [12].

4.2 CONSEQUENCES OF DEPLOYING DEFAULT CONFIGURATIONS

Departments can help harden their operating systems by deploying Windows 10 with updated configurations, leveraging the robust suite of security features as listed in Table 1 above. From a security perspective, the default (i.e. out-of-the-box) configuration of Windows 10 does not meet the required level of security for GC departments. If the default configuration is used, we strongly recommend that departments implement the security features outlined in this document and the baseline settings detailed in the *GC Security Baseline for Windows 10* [1].

5 GPO SETTINGS

Working with SSC, we have established baselines for GPO settings in Windows 10 (release 1607). These settings fall into two categories: minimum baseline settings and additional enhanced baseline settings. See Section 8.1 for instructions on how to get a copy of the *GC Security Baseline for Windows 10* [1], which details the settings for these baseline configuration.

To establish these settings, we consulted configuration guidance publications developed by other organizations:

- Center for Internet Security (CIS) – *Securing Microsoft Windows Desktop* [13]
- Defense Information Systems Agency (DISA) - *Windows 10 Security Technical Implementation Guide* (STIG) [14]
- Microsoft Security Guidance Blog – *Security Baseline for Windows 10 v1607 ("Anniversary Edition") and Windows Server 2016* [15]

5.1 MINIMUM BASELINE SETTINGS

The minimum baseline settings are required for GC departments. These settings are considered mandatory for GC departments because they provide most endpoint devices with the level of security required to protect GC information assets and infrastructure against threats.

These settings are labelled as "Minimum Baseline" in the *GC Security Baseline for Windows 10* [1]. Certain settings have been selected to hard code them. Although the same effect of hard coding could have been achieved by keeping them as "not configured", selecting the settings better reflects the baseline and enables a level of control for future automatic and recommended updates that may need to be reviewed prior to implementation.

5.2 ENHANCED BASELINE SETTINGS

The enhanced baseline settings are operating system settings specific to supporting Protected B environments. The enhanced baseline settings, along with additional security requirements not covered in this document, are required to provide additional security for sensitive information. These settings are labelled as "Enhanced Baseline" in the *GC Security Baseline for Windows 10* [1].

6 GPO IMPLEMENTATION WORKAROUNDS AND FIXES

Several Windows 10 workarounds and fixes, which are specific to release 1607, are listed in the subsections below.

6.1 FIPS MODE

Recommendation: Enable FIPS mode.

The FIPS mode option should be enabled and used in Windows 10. Only CCCS-approved (and therefore FIPS-approved) algorithms should be used for securing sensitive information. The algorithms are inherent to the FIPS mode functionality.

Application testing should be conducted to determine that Windows 10 can function properly in FIPS mode for a given environment. If there are any issues or concerns, call the CCCS Contact Centre for assistance.

6.2 PEER-TO-PEER

Recommendation: Peer-to-peer networking services should not be configured (i.e. the default setting).

The "Turn off Microsoft Peer-to-Peer Networking Services" GPO setting originated in Windows XP. This setting intended to lock down specific capabilities, such as real-time communications (e.g. server-less instant messaging, real-time matchmaking, and game play), Windows Meeting Space collaboration, content distribution, and distributed processing. For more information, see *Introduction to Windows Peer-to-Peer Networking* [16].

Modern peer-to-peer technologies that emerged after Windows XP, such as Windows BranchCache (peer-to-peer mode), ConfigMgr (1610+) Peer Cache, and Windows 10 Updates Delivery Optimization, are critical to the cost-effective deployment and lifecycle maintenance (i.e. patching, software installation, and Windows servicing) of Windows 10-based desktop devices. These peer-to-peer technologies can reduce requirements for expensive server equipment at each location with sub-optimal bandwidth.

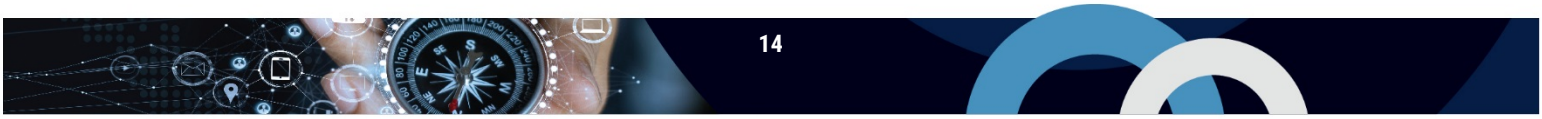
There should be no impact if the setting is turned on. The setting applies to the legacy Peer Name Resolution Protocol (PNRP) grouping and Graphing and People Near Me protocols, which are still used for HomeGroup. For example:

- Windows Updates Delivery Optimization (WUDO) and BranchCache are not affected because they are built on different components.
- ConfigMgr Peer Cache is not affected because Peer Cache discovery is managed by ConfigMgr Management Points, and content delivery is done over hypertext transfer protocol (HTTP) and HTTP secure (HTTPS).

6.3 POWERSHELL

There is no supported ability to disable PowerShell[8]. It has become a critical component of the operating system and many applications. However, there are several ways to lock it down slightly for non-privileged users. Consider the following:

[8] PowerShell is the current command shell for Windows. Since release 1511 of Windows 10, PowerShell has been the default command shell, supplanting the Windows NT-era Command Prompt (i.e. CMD.EXE).



- Any PowerShell script will only execute with the same permissions as the user or process launching the script.
- Windows 10 ships with PowerShell 5.0, which is a considerably more secure iteration of PowerShell with more logging and detection capabilities than its predecessors. These capabilities are described in *Advances in Scripting Security and Protection in Windows 10 and PowerShell V5* [17].
- PowerShell has numerous execution policy levels that can be set by GPO, as described in *About Execution Policies* [18]. See Table 2 for a description of the execution policy levels.
- Devices should be configured at either the **Restricted** or **AllSigned** level for maximum security and flexibility.

Table 2: PowerShell Execution Policy Levels

Execution Policy Level	Description
Restricted Level	• Default execution policy in Windows 8, Windows Server 2012, and Windows 8.1. • Permits individual commands, but will not run scripts. • Prevents running of all script files, including formatting and configuration files (.ps1xml), module script files (.psm1), and Windows PowerShell profiles (.ps1).
AllSigned Level	• Scripts can run. • Requires all scripts and configuration files to be signed by a trusted publisher, including scripts that you write on the local computer. • Prompts you before running scripts from publishers that you have not yet classified as trusted or untrusted. • Risks running signed but malicious scripts.
RemoteSigned Level	• Scripts can run. This is the default execution policy in Windows Server 2012 R2. • Requires a digital signature from a trusted publisher on scripts and configuration files that are downloaded from the Internet (including email and instant messaging programs). • Does not require digital signatures on scripts that you have written on the local computer (not downloaded from the Internet). • Runs scripts that are downloaded from the Internet and not signed if the scripts are unblocked (e.g. by using the Unblock-File cmdlet). • Risks running unsigned scripts from sources other than the Internet and signed but malicious scripts.
Unrestricted Level	• Unsigned scripts can run. This risks running malicious scripts. • User warned before scripts run and configuration files are downloaded from the Internet.
Bypass Level	• Nothing is blocked. There are no warnings or prompts. • This execution policy is designed for configurations in which a Windows PowerShell script is built into a larger application or in which Windows PowerShell is the foundation for a program that has its own security model.

6.4 SLEEP MODE IN TABLETS

Recommendation: Use the sleep mode settings listed in Table 3.

Table 3: Recommended Sleep Mode Settings

Setting	Minimum Baseline	Enhanced Baseline
Allow standby states (S1-S3) when sleeping (on battery)	Disabled	Enabled
Allow standby states (S1-S3) when sleeping (plugged in)	Disabled	Enabled
Specify the system sleep timeout (on battery)	Not configured	Enabled
Specify the system sleep timeout (plugged in)	Not configured	Enabled

Windows 10 supports several sleep states for compatible devices, as described in *System Sleeping States* [19]. The four states that are most commonly encountered on modern hardware are:

- S0 (system working)
- S3 (sleep)
- S4 (hibernation)
- S5 (system shutdown)

> **Note:** States S1 and S2 are not detailed in the table below because the issues discussed do not affect these states. For further information on states S1 or S2, refer to *System Sleeping States* [20].

When a device is encrypted with BitLocker using the TPM+PIN protector, only those devices starting from a powered-off state (S4 or S5) will be prompted for a PIN. Systems waking from other sleep states, such as S3, will proceed directly to the lock screen without a PIN prompt.

The Group Policy setting "\System\Power Management\Sleep Settings\Require a password on wakeup" is used to enforce whether the user must re-authenticate before returning to their user session.

Table 4: Tablet Sleep Modes

Sleep State	Configuration/Characteristics
System Working State S0	**Power consumption** Maximum. However, the power state of individual devices can change dynamically as power conservation takes place on a per-device basis. Unused devices can be powered down and powered up as needed.

Sleep State	Configuration/Characteristics
	Software resumption Not applicable. **Hardware latency** None. **System hardware context** All context is retained.
System Power State S3	**Power consumption** Less consumption than in state S2. Processor is off, and some chips on the motherboard might be off. **Software resumption** After the wake-up event, control starts from the processor's reset vector. **Hardware latency** Almost indistinguishable from state S2. **System hardware context** Only system memory is retained. CPU context, cache contents, and chipset context are lost.
System Power State S4 System power state S4, the hibernation state, is the lowest-powered sleep state and has the longest wake-up latency. To reduce power consumption to a minimum, the hardware powers off all devices. However, operating system context is maintained in a hibernation file (an image of memory) that the system writes to disk before entering the S4 state. Upon restart, the loader reads this file and jumps to the system's previous pre-hibernation location. If a computer in state S1, S2, or S3 loses all AC or battery power, it loses system hardware context, and therefore, must reboot to return to S0. A computer in state S4 can restart from its previous location even after it loses battery or AC power because operating system context is retained in the hibernation file. A computer in the hibernation state uses no power (with the possible exception of trickle current).	**Power consumption** Off, except for trickle current to the power button and similar devices. **Software resumption** System restarts from the saved hibernation file. If the hibernation file cannot be loaded, rebooting is required. Reconfiguring the hardware while the system is in state S4 might result in changes that prevent the hibernation file from loading correctly. **Hardware latency** Long and undefined. Only physical interaction returns the system to the working state. Such interaction might include the user pressing the ON switch or, if the appropriate hardware is present and wake-up is enabled, an incoming ring for the modem or activity on a LAN. The machine can also awaken from a resume timer if the hardware supports it. **System hardware context** None retained in hardware. The system writes an image of memory in the hibernation file before powering down. When the operating system is loaded, it reads this file and jumps to its previous location.
System Shutdown State S5 In state S5, or shutdown state, the machine has no	**Power consumption** Off, except for trickle current to devices such as the power button.

Sleep State	Configuration/Characteristics
memory state and is not performing any computational tasks. The only difference between states S4 and S5 is that the computer can restart from the hibernation file in state S4, while restarting from state S5 requires rebooting the system.	**Software resumption** Boot is required upon awakening. **Hardware latency** Long and undefined. Only physical interaction, such as the user pressing the ON switch, returns the system to the working state. The BIOS can also awaken from a resume timer if the system is so configured. **System hardware context** None retained.

7 CONTINUOUS EVOLUTION, RELEASES, AND VERSIONING

The guidance in this document forms foundational baseline elements to help harden Windows 10 operating systems. This document outlines the GPO settings and operations according to release 1607 of Windows 10.

At the time of this document's publication, the security features and tools listed in this document are Microsoft's most recent service offerings for Windows 10 (release 1607). Microsoft indicated that continuous improvements will be made to Windows 10. New releases are expected to occur in six-month increments. This document may be updated to ensure all relevant security features and tools are captured. Significant changes or additions to the workarounds and fixes described in this document will be released as addendums.

8 SUMMARY

Windows 10 provides updated security features and tools. These security features and tools should be used to develop a secure common desktop operating environment for GC departments. To get a copy of the detailed GPO settings, see Section 8.1 below. We worked with SSC and authorities from Microsoft Canada to establish these GPO settings. Both the minimum and enhanced baseline settings align with GC IT security requirements.

While these baselines are a mandatory component of achieving a common security posture for all GC endpoint devices, some deviations or modifications may be required to accommodate departmental business needs and security requirements that are identified in completed TRAs. All resulting requirements should be properly documented.

8.1 CONTACTS AND ASSISTANCE

If additional information or guidance is needed, call the CCCS Contact Centre.

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

To get a copy of the latest version of *GC Security Baseline for Windows* [1], send an email to SSC at the following address:

SSC.DesktopOSImaging-ImagedesSOdetravail.SPC@canada.ca

GC departments can also get a copy through GCconnex. Subscribe to the WTD Common Desktop Operating Environment GCconnex group.

9 SUPPORTING CONTENT

9.1 LIST OF ABBREVIATIONS

Term	Definition
AMD-V	Advanced Micro Dynamics Virtualization
BIOS	Basic Input / Output System
CIS	Center For Internet Security
CMVP	Cryptographic Module Validation Program
COMSEC	Communications Security
CSE	Communications Security Establishment
DCM	Desired Configuration Manager
DISA	Defense Information Systems Agency
EMET	Enhanced Mitigation Experience Toolkit
FIPS	Federal Information Processing Standards
GC	Government Of Canada
GPO	Group Policy Object
GUID	Global Unique Identifier
HTTP/HTTPS	Hypertext Transfer Protocol / HTTP Secure
HVCI	Hypervisor Code Integrity
ISSIP	Information System Security Implementation Process
IT	Information Technology
ITS	Information Technology Security
MBR	Master Boot Record
MOICE	Microsoft Office Isolated Conversion Environment
NTLM	New Technology Local Area Network Manager
PNRP	Peer Name Resolution Protocol
SCM	Software Compliance Management
SLAT	Second Level Address Translation
SSC	Shared Services Canada
SSDCL	Secure Systems Development Lifecycle Process
STIG	Security Technical Implementation Guide

Term	Definition
TBS	Treasury Board of Canada Secretariat
TPM	Trusted Platform Module
TRA	Threat and Risk Assessment
UEFI	Unified Extensible Firmware Interface
VT-x	Intel Virtualization Technology
WUDO	Windows Updates Delivery Optimization

9.2 REFERENCES

Number	Reference
1	Shared Services Canada *GC Security Baseline for Windows*.
2	Communications Security Establishment. *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information.* October 2017.
3	Treasury Board of Canada Secretariat. *Policy on Management of Information Technology.* July 2007.
4	Treasury Board of Canada Secretariat. *Policy on Government Security.* July 2009.
5	Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology.* May 2004.
6	Treasury Board of Canada Secretariat. IT Policy Implementation Notice (ITPIN). *Direction on Windows 10 Desktop Operating System Migration and Configuration*. 10 August 2018.
7	Communications Security Establishment. *ITSG-33 IT Security Risk Management: A Lifecycle Approach.* December 2014.
8	Microsoft. *Device Security.* 4 May 2017.
9	Microsoft. *Features that are Removed or Deprecated in Windows 10 Fall Creators Update.* 12 December 2017.
10	Communications Security Establishment. *ITSB-95 Application Whitelisting Explained*. March 2015.
11	Microsoft. *Ensure Device Compliance with System Center Configuration Manager*. 6 October 2016.
12	Microsoft. *What is Protected View?* N.D.
13	Center for Internet Security (CIS). *Microsoft Windows Desktop CIS Benchmark*. N.D.
14	Defense Information Systems Agency (DISA). *Windows 10 Security Technical Implementation Guide (STIG)*. 18 August 2017.
15	Microsoft. *Security Baseline for Windows 10 v1607.* 17 October 2016.
16	Microsoft. *Introduction to Windows Peer-to-Peer Networking*. 27 September 2006.

Number	Reference
17	Microsoft. *Advances in Scripting Security and Protection in Windows 10 and PowerShell V5*. 10 June 2015.
18	Microsoft. *About Execution Policies*. N.D.
19	Microsoft. *System Sleeping States*. 16 June 2017.