# System Security Standard

**CWB Financial Group – Information Security Office**

**Document Version V1.0**

**May 20, 2020**

CWB
Financial Group

# Contents

# Document Summary

## Introduction

CWB Financial Group (herein referred to as CWBFG) requires all CWBFG systems to be acquired and configured with information security requirements in mind. Only systems owned or managed by CWBFG that have been sufficiently hardened, can be connected to CWB Financial Group's network. Adhering to this standard will reduce the security risks and protect systems from attacks against known/zero-day vulnerabilities found in operating systems, application software and firmware.

As per the CWBFG ***Information Security Logical Architecture***, this standard supports the following principles:

- Zero Trust
- Defense in Depth
- Protection of Information Assets
- Assurance of Correct and Reliable Operation
- Defense Against Threats
- Defense Against Fraud

## Purpose

The intention of this document is to provide the security requirements for CWBFG systems using a collection of tools, techniques, and hardening best practices. This standard will ensure effective controls are implemented to protect the confidentiality, integrity and availability of CWBFG data exposed by these assets. Hardening practices require on-going monitoring for deviations and continuous maintenance. The expected benefits include:

- improved security – where a reduced attack surface can improve the availability of assets, and lowers the risk of cybersecurity breaches, unauthorized access, hacking or malware;
- enhanced functionality – where fewer services and function reduce the risk of operational issues, misconfiguration, incompatibilities, and compromise; and
- reduced compliance and audit efforts– where the assessment of a consistently hardened, less complex environment will be more transparent and straightforward.

## Scope

This standard is applicable to all Information Owners and Information Custodians (e.g. Application Support teams, Data Centre teams, and third-party service providers) who support CWBFG owned and network-attached systems including on premise, cloud based or vendor-based systems.

This standard includes the following topics:

- System Acquisition, Protection & Use
- System Configuration Management
- System Communication Protection
- System Vulnerability and Patch Management

## Out of Scope

This standard does not include detailed configuration settings for each type of system, instead links have been provided to best practices or industry standards to ensure the latest baseline configuration information is referenced.

# Standard Statements

## System Acquisition, Protection & Use

System acquisition is the process of assuring that adequate controls are considered, evaluated, selected, designed and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation and operation stages.

### General Requirements

- Information Owners and Information Custodians must:
  - ensure that systems, software and firmware are obtained from trusted sources.
  - document organization-wide system hardware, firmware and software acquisition controls.

**For system acquisition activities, the Information Custodians must:**

- follow department defined system acquisition documentation that includes standard hardware and software requirements;
- allocate resources required to protect CWBFG systems and data, as part of its operational planning process;
- manage systems using a System Development Life Cycle (SDLC) that incorporates information security controls, including:
  - secure configuration, installation, and operation of the system;
  - effective use and maintenance of security features/functions;
  - remediation of known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions;
  - user-accessible security features/functions and how to effectively use those security features/functions;
  - methods for user interaction with the system, which enables individuals to use the system in a more secure manner;
  - obtaining sign-off prior to promoting a system into production; and
  - ongoing responsibilities in maintaining the security of the system and information.
- follow formal testing and acquisition process, when purchasing systems or outsourcing hardware, including:
  - establishing a segmented lab environment that provides a safe environment to execute potentially hostile commands/executables or test applications;
  - ensuring vendors provide documentation describing the functional properties of the security controls employed within systems, system components, or system services in sufficient detail to permit risk analysis and security testing of the controls; and
  - ensuring contracts with the supplier address the identified security requirements.

**For software acquisition activities, the Information Custodians must:**

- require third parties (e.g. developers, vendors and service providers) to adhere to the ***Third Party Standard***, and must:
  - provide documentation describing the design and implementation of security controls employed within software components or services in sufficient detail to permit risk analysis and security testing of the controls;
  - demonstrate that their software development processes employ:
    - industry-recognized leading practices for secure coding (e.g. code reviews, use code analysis tools, etc.);
    - secure engineering methods;
    - quality control processes; and
    - testing processes to minimize flawed or malformed software.
- prioritize the selection of Commercial off the Shelf (COTS) software over open-source (in alignment with Enterprise Architecture TEP02 principle), when there is:
  - assurance matters, such as business critical applications;
  - sensitive data such as Personally Identifiable Information (PII) involved and where the ***Data Protection Standard*** compliance is mandated by the Information Security Office;
  - no on-going software developer support;
  - software which requires on-going driver support;
  - a choice between a well established closed source vendor and a small Commercial Open Source Software (COSS) vendor which can include service warranty and legal indemnity matters; and
  - a new information security service is to be implemented.
- require third-party developers of information system, system component, or information system service to provide that evidence of independent third party assessment of security control effectiveness in the service they are providing.
- require identification of all security functions, ports, protocols, and services that must be enabled for use in a production environment. This will also include documentation describing external system interfaces (e.g., data connections).
- provide documentation in sufficient detail to permit risk analysis and an architectural review.

# System Baseline Configuration Management

Baseline Configuration Management is the practice of standardizing the configuration of similar assets based upon best practice security requirements. The configuration of a system and its components has a direct impact on CWBFG's overall security posture, and how system baseline configurations are established and maintained requires a disciplined approach for providing adequate security.

CWBFG System types include:

- End User Computing (EUC) devices: laptops, Surfaces, workstations, mobile devices; and
- Technology Assets (e.g. servers, security services, hardware appliances, etc.).

## General Requirements

- Systems must be sufficiently hardened incorporating the security principle of 'Least Functionality' (CM-7), where:
  - baseline configuration management activities are defined and maintained to protect against improper modification prior to, during and after asset implementation;
  - baseline configurations should be developed and implemented in a top-down approach to ensure consistency across CWBFG. An example is the implementation of the group policy functionality, which can be used to distribute secure configuration policy in a centralized manner throughout established domains. (CM-1; CM-6)
  - exceptions must be documented for configurations not following global industry benchmarks or vendor best practices. These exceptions must be reviewed and approved by the Information Security Office.
- Where technically feasible, separate physical or logical storage space must be implemented, this includes:
  - Database installation directory/drive;
  - Application installation directory/drive; and
  - User Directory/Location

**Information Owners and/or Information Custodians**

Accountable and responsible for:

- establishing baseline configurations. For each type or category of system, leverage global industry benchmarks, which reflect the most restrictive mode consistent with operational requirements. It is not expected every system will be 100% compliant with these benchmarks, but it is expected any gaps are reviewed with the Information Security Office, so it can be decided if a risk exception must be granted. CWBFG recommends the following global industry benchmarks:
  - **Center of Internet Security (CIS) Benchmarks** ( https://www.cisecurity.org/cis-benchmarks/ ) by enforcing at a minimum, level 1 configuration settings and associated group policies; or
  - **NIST Security Configuration Checklists** ( https://nvd.nist.gov/ncp/repository ), when a CIS benchmark is not available for a given asset (CM-6); and
  - **Vendor/supplier configuration best practice guides** when no CIS or NIST relevant benchmarks are available.
    - For CWBFG Linux Systems: Red Hat Satellite will leverage Ansible and OpenSCAP for system hardening.

- hardening all systems and seeking signoff from the Information Services prior to use and prior to promotion to production. Leverage established benchmarks to harden all systems types, in all environments (e.g. production, test and development) using security configuration checklists or standard images, for:
  - **Servers**: Established via VM Image templates and Azure ARM templates, including:
    - Domain Controllers
    - Member Servers (e.g. DHCP, DNS, File Server, Hyper-V, Print, Remote Desktop, Web servers)
  - **EUC**: Established via Gold images, MDM, iPhone apple updates) , including:
    - Laptops
    - Surfaces
    - Desktops
    - Mobile Phones
- keeping the operating system service release, service packs and patches up to date. Other considerations include:
  - operating system service at N-1 release (which equates to the prior stable version) is acceptable, when there are no major or critical security vulnerabilities to address;
  - there may be situations where the application is auto-updated to the latest version (e.g. Google Chrome) on a regular basis;
  - managing operating system-independent applications, based on the threat they may pose, since they can run on multiple operating systems; and
  - uninstalling operating system-independent applications from systems where the applications are not required for a business purpose such as Public store, Windows Defender etc.
- implementing configuration standards for all system components that address known security vulnerabilities and are consistent with industry-accepted system hardening standards (Refer to Appendix B - Benchmarks);
- setting secure operating system policies (i.e. the parameters that describe how particular automated functions of IT products behave). For Windows systems enforce hardening of servers via Group Policy (GPO). This will ensure the hardening settings are re-applied after any changes are made as result of an application installation. These settings include, but not limited to:
  - Group Policy Objects (GPO), including:
    - account policies, including password and account lockout policies; and
    - local policies, including audit and user rights assignment policies;
  - Security Options, including accounts, audit, devices, domain controller, domain member, interactive logon, network client, network server, network access, network security, and user account control, etc.;
  - Windows Firewall policies, including domain, private and public profiles;
  - advanced audit policies, including account logon/logoff, account management, policy change, privilege use;
  - admin templates computer and user policies, including Local Admin Password Solution (LAPS), encrypted OS drives, removable data drives, screen savers, USB device restrictions, etc.; and
  - All GPOs must be reviewed at least annually.

- limiting the implementation of software applications to only those software applications required by the business.
- implementing the following security software on all systems. Ensuring automatic updates are configured, to keep data protection mechanisms current:
  - GlobalProtect Agent;
  - FireEye Endpoint Detection and Response agents;
  - Okta Browser Plugin;
  - BitLocker HDD encryption for laptops/surfaces; and
  - SCCM Agent.
- ensuring systems are configured to require privilege levels of access. These levels must ensure data is not exposed to individuals or processes with a lower privilege level.
- tailoring secure configurations according to systems function and role (CM-6; RA-3);

  For critical systems:
  - deploy application whitelisting to alert Information Security Operations personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons periodically; and
  - verify the use of application whitelisting tools by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored:
    - system executables;
    - application executables;
    - configuration and parameter files; and
    - centrally stored, historical or archived, log and audit files.
- storing baseline configurations in a secure location and/or on read only media when used for daily operations. This will prevent threat actors from making modifications to baseline configurations;
- reviewing and updating the baseline configurations over time, as enhancements or upgrades are made, including:
  - conducting on-going monitoring and detection of baseline deviations, including unnecessary and/or non-secure functions, ports, protocols, services and applications. CIS benchmark testing tools and vulnerability scans help to identify deviations to established baseline configuration; and (CM-2)
  - remediating any identified benchmark gaps, or documenting any exceptions for the Information Security Office's approval. (CM-2)
- ensuring configuration changes are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation, to maintain the approved baseline. (CM-3 - 2.18.2). This includes:
  - assessing changes to a system after a change has been implemented to ensure correct operation and that there were no deviations;
  - requesting a risk assessment to be performed on all major changes that could affect security, including configuration changes, the addition of network components, and installation of new software; and
  - retaining a record of configuration-managed changes.

- ensuring the availability of system components (hard drives, power supply, monitor, etc.) by taking proactive steps to prevent downtime associated with predictable failures; and
- physically disabling, removing connection ports, or input/output devices on sensitive systems (e.g. disable the use of USB Ports in order to prevent data loss).

**Information Security Office (ISO)**

Responsible for:

- reviewing baseline configurations, as required as part of compliance or risk assessments activities;
- advising Owners on the mandatory baseline configuration settings;
- reviewing the documented exceptions to benchmark configuration settings. Exceptions can be processed by the Information Security Office, and usually only granted on a case-by-case basis for a limited time-period;
- ensuring that system protection mechanisms are actively running and cannot be disabled or altered by users;
- verifying the Endpoint Detection and Response (EDR) service is configured to alert Information Security Operations personnel when unauthorized modification of critical files on all systems is detected; and
- responding to EDR and application whitelisting tools alerts.

## System Communication Protection

CWBFG requires communication functions, ports, protocols, and services to be controlled and maintained. For situation awareness, such information can be useful when the need arises to quickly understand the trade-offs involved in blocking specific ports, protocols, or services or when requiring external service providers to do so.

### General Requirements

- CWBFG is required to document organization-wide system communication controls that, at a minimum, include:
  - use of trusted sources for authoritative DNS queries on all systems to prevent DNS spoofing attacks, including:
    - Internal DNS Servers;
    - Shaw DNS Servers; and
    - Telus DNS Servers.
- Information Services are required to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following criteria is implemented for acquiring, distributing, and storing time:
  - critical systems have the correct and consistent time;
  - time data is protected; and
  - time settings are received in following order:
    - Internal NTP Server (ntp.cwb.local); and then
    - Industry-accepted time sources for public services.

- Secure cryptographic mechanisms (TLS 1.2 or higher) must be implemented to prevent unauthorized disclosure and modification of information on information system components. If there are technical constraints preventing the implementation of this requirement, use the risk exception process to document the exception.
- Requests for non-standard communication technologies must be approved by the Information Security Office, prior to implementation. Information Services will install the following approved communications technologies:
  - Electronic Mail (email) – Office 365;
  - Instant Messaging (IM) – Microsoft Teams, Skype for Business;
  - Voice Over Internet Protocol (VOIP) – TC2 Telus Service;
  - Facsimile (Fax) Machines (analog & digital) - Rightfax;
  - Printers – Cirrato Printer services, Xerox and HP; and
  - Cheque Imaging - Panini cheque scanners.

## System Vulnerability and Patch Management

**Vulnerability Management**

Vulnerability assessments are point in time exercises intended to identify and analyze weaknesses or flaws associated with systems. Vulnerability remediation management is the practice of evaluating identified vulnerabilities and planning an appropriate response. Vulnerability analysis can help to assess the effectiveness of baseline configurations and help to identify software releases, fix packs or patches that may be missing.

**Patch Management**

Patch management is a practice designed to proactively prevent the exploitation of vulnerabilities that exist on Information Technology Assets. By applying security related software or firmware updates (patches), the expected results can reduce the probability that existing flaws can be exploited, and can save time, effort and costs responding to newly reported vulnerability-related incidents. (CM-2, CM-3, CM-4, SI-2)

As patches greatly impact the secure configuration of a system, the patch management process is integrated into configuration management, including:

- performing security impact analysis of patches;
- testing and approving patches as part of the configuration change control process;
- updating baseline configurations to include current patch level;
- assessing patches to ensure they were implemented properly; and
- monitoring systems/components for current patch status.

Detailed Vulnerability Management and Patch Management requirements are described in detail within the ***Vulnerability Management Standard***.

# Exceptions

All exceptions to this standard must be documented and approved by both the Information Owner and the Chief Information Security Officer. Exceptions to this standard must be documented and registered as a risk as per the Information Security Governance, Risk, and Compliance processes. Identified risks must be assessed by the CWBFG Information Security Office and mitigated in partnership with the business owner and third-party service providers.

# Enforcement

Failure to comply with this standard may impact the business and reputation of CWBFG. Depending on the circumstances, CWBFG will act to correct violations of this standard through training, counselling, disciplinary action, termination of employment, civil action or criminal prosecution.

It is the policy of CWBFG to handle information security incidents so as to minimize their impact on the confidentiality, integrity, and availability of CWB information systems, applications, and data. An information data breach incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information that interferes with information technology operations. All such incidents must be reported to the CWBFG Information Security Office.

# Roles and Responsibilities

| Role | Responsibility |
|---|---|
| Chief Information Security Officer | • Accountable for the creation, maintenance, and implementation of this standard where applicable.<br>• Accountable to have and maintain written standards and procedures necessary to ensure implementation of and compliance to this standard.<br>• Accountable to provide appropriate support and guidance to assist employees to fulfill their responsibilities of complying with this standard. |
| Sr. Manager, Information Security Program Management | • Responsible for the creation and maintenance of this standard and supporting policy where applicable.<br>• Responsible to have and maintain written standards and procedures necessary to ensure implementation of and compliance to this standard.<br>• Responsible to provide support and guidance to assist employees to fulfill their responsibilities of complying with this standard.<br>• Consulting with the Sr. Manager, Security Governance, Risk and Compliance and the Sr. Manager, Security Operations, as required. |
| CWBFG's Executive Leadership Team, Senior Leadership Team, Directors, and Managers | • Understand and comply with this standard and supporting policy in its entirety.<br>• Responsible to create and maintain processes and procedures to support this standard and supporting policy.<br>• Responsible to ensure that all appropriate personnel are aware of and comply with this this standard and supporting policy.<br>• Responsible for the creation of appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this standard and supporting policy. |
| CWBFG employees, contractors, third-party service provider, etc. | • Understand and comply with this standard and supporting policy in its entirety.<br>• Implement this standard with supporting processes and procedures.<br>• Report vulnerabilities and breaches. |

# Appendix A – Document Control

**Document Status**

| | |
|---|---|
| **Document Name** | System Security Standard |
| **Document Owner** | Chief Information Security Officer |
| **Version** | Version 1.0 |
| **Publication Date** | |
| **Information Classification** | Internal Use |
| **Revision Status** | Final |
| **Custodian** | Sr. Manager, Information Security Program Management |
| **Organization** | CWBFG Information Security Office |
| **Retention Period** | Retain for ongoing use |
| **Master Storage Location** | |

**Revision History**

| Version | Author | Contributor | Description of Changes |
|---|---|---|---|
| Draft 0.1 | Joanne Pearson | Vikram Singh | Document creation |
| Draft 0.2 | Vikram Singh | Joanne Pearson | Updates made after initial review. |
| Draft 0.3 | Joanne Pearson | Vikram Singh | Formatting changes after joint review |
| Draft 0.4 | Vikram Singh | Joanne Pearson | Appendix changes<br>Request for Feedback sent to:<br>• Thomas Matthews<br>• Jose Barrill<br>• Reinhardt Tonn |
| Draft 1.0 | Joanne Pearson | Thomas Matthews | Feedback provided on previous draft – Ready for CISO review. |
| Final V1.0 | Joanne Pearson<br>Vikram Singh | Cory Gould/CISO | Feedback incorporated – published in Keylight |

# Appendix B – Hardening Benchmarks

Common baseline configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, and security technical implementation guides) provide recognized, standardized, and established benchmarks. These benchmarks stipulate specific settings for information technology platforms/products and provide configuration instructions to meet operational requirements. *Table 1* below highlights the common systems deployed and the global industry benchmarks that can be leveraged.

***Table 1: Hardening Benchmarks***

| Configuration Benchmark | SharePoint Link |
|---|---|
| **Server Operating System** | |
| Microsoft Server 2016 Domain Controller and Member Servers | CIS Benchmark - Windows Server 2016 |
| Red Hat Linux 7 & 8 | CIS Benchmark - Red Hat Linux 7 & 8 |
| **Server Software – Web Server** | |
| Microsoft IIS 10 | CIS Benchmark - IIS 10 |
| Apache Tomcat | CIS Benchmark - Tomcat |
| **Server Software - Virtualization** | |
| VMware | CIS Benchmark - VMware ESXi |
| **Server Software - Collaboration Server** | |
| Microsoft SharePoint | CIS Benchmark -SharePoint |
| **Server Software - Productivity** | |
| Microsoft Exchange Servers | CIS Benchmark - Exchange Server |
| **Server Software - Virtualization** | |
| VMware | CIS Benchmark - VMware ESXi |
| **Server Software - Collaboration Server** | |
| Microsoft SharePoint | CIS Benchmark -SharePoint |
| **Server Software - Productivity** | |
| Microsoft Exchange Servers | CIS Benchmark - Exchange Server |
| **Server Software – Database Servers** | |
| Microsoft SQL Server 2016 | CIS Benchmark - SQL Server 2016 |
| Oracle Database Server | CIS Benchmark - Oracle Database |
| PostgreSQL Database Server | CIS Benchmark - PostgreSQL |
| Oracle MySQL Database server | CIS Benchmark - Oracle MySQL |
| **Network Devices** | |
| Palo Alto Firewalls | CIS Benchmark - Palo Alto Firewall |
| Cisco Devices | CIS Benchmark - Cisco Devices |
| **Desktop – Operating System** | |

| Configuration Benchmark | SharePoint Link |
|---|---|
| Microsoft Windows 10 | CIS Benchmark Windows 10<br><br>Windows 10 Security Recommendations |
| **Desktop - Applications** | |
| Google Chrome | CIS Benchmark - Google Chrome<br><br>Google Chrome Security Recommendations |
| Microsoft Internet Explorer 11 | IE 11 Security Requirements |
| Firefox | CIS Benchmark Firefox 38 ESR |
| Microsoft Office 2016 | Office 2016 Security Recommendations |
| Microsoft BitLocker | BitLocker Benchmark |
| Print Devices | CIS Benchmark - Printers |
| **Desktop – Antivirus** | |
| Microsoft Windows Defender | Windows Defender Benchmark for Workstations |
| **Mobile Devices** | |
| Apple IOS | CIS Benchmark - IOS |
| Safari Browser | CIS Benchmark - Safari |

# Appendix C – Authorized Operating Systems

The following operating systems have been approved for use in the CWBFG environments:

| System | Operating System |
|---|---|
| **Desktop, Surface, Laptop** | Windows 10 |
| **Windows Servers** | Windows Server 2019<br>Windows Server 2016<br>Windows Server 2012 R2<br>Windows Server 2012 |
| **Linux Server** | RHEL 7.6<br>RHEL 7.5<br>RHEL 7.4 |
| **Mobile Phone (iPhone)** | iOS 13<br>iOS 12<br>iOS 11.2 |
| **iPad** | iOS 13<br>iOS 12<br>iOS 11.2 |

# Appendix D - Definitions

The following table highlight key definitions used in this Standard.

| | |
|---|---|
| **CISO** | Chief Information Security Officer |
| **CWBFG** | Canadian Western Bank Financial Group |
| **EDR – System Detection and Response** | A security service that continuously monitors and responds to mitigate cyber threats. It can also be known as an Endpoint Protection Solution that focuses on advanced persistent threats. |
| **Patch Management** | The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions, known as patches, hot fixes and service packs. |
| **System Acquisition** | The process of assuring that adequate controls are considered, evaluated, selected, designed and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation and operation stages. |
| **System Baseline Configuration** | A documented set of specifications for an information system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. |
| **System Communication Protection** | Is the application of communications security measures enabled to deny unauthorized access to sensitive unclassified information of value, prevent disruption of services, or (c) ensure the authenticity of information handled by the stems. |
| **Vulnerability Management** | An information security continuous monitoring capability that identifies vulnerabilities or weakness on assets that are likely to be used by threat actors to compromise an asset and use it as a platform form which to extend compromise to the network. |