Network Access Standard

CWB Financial Group – Information Security Office

Document Version: V 1.0

May 25, 2020

Contents

Document Summary

Introduction

CWB Financial Group (herein referred to as CWBFG) requires all network access methods to be managed and controlled, to ensure the protection of CWBFG information and all its supporting information processing facilities.

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

- Zero Trust
- Defense in Depth
- Compartmentalization
- Access Control
- Protection of Information Assets
- Defense Against Threats

Purpose

The purpose of this standard is to document the requirements for network segmentation, and the network access methods used to access CWBFG's wired, wireless networks and key network services (e.g. remote access and mobile device access).

Scope

This standard applies to all individuals who use, provision, and support CWBFG's technology assets, regardless of where these assets are located (e.g. Corporate or Cloud Service Providers). This also applies to authorized third parties who use or provide services, manage, or support CWBFG's technology assets.

As a cloud service customer, this standard also applies to the methods used to design and create the physical and virtual networks used to deliver service from the cloud service providers our business engages with.

The Network Access Standard includes the following topics:

- Network Access – General Requirements
- Security Zones
- Remote Network Access
- Third Party Network Access
- Wireless Access
- Mobile Device Access

Out of Scope

This standard does not include requirements for information flow control services, instead please refer to the ***Information Flow Control Standard*** for the following services:

- Firewall
- Azure Network services (e.g. Network Security Groups)
- Gateways/Proxies/Load Balancers (Email, Web, Access Portals)
- Web Application Firewalls (WAFs)
- Web Content Filtering

Standard Statements

Network Access

Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to information systems that use the network, some of which require protection from other network access because of their sensitivity or criticality.

Unauthorized and unsecured connections to network services can negatively affect CWBFG's ability to protect information from disclosure, alteration or made unavailable. This requirement is especially important for network connections to sensitive or critical business applications, or for authorized individuals accessing the internal network from un-trusted networks.

General Requirements

- All CWBFG managed devices accessing the CWBFG's network must follow the network access requirements provided in this standard. This also includes all non-CWBFG managed devices that have been authorized to access CWBFG networks.
- All new network access methods used to access CWBFG network, services, systems, applications and information must be authorized by the VP of Information Services and the Chief Information Security Officer.
  - When unauthorized devices, systems and services are detected, a network access control (NAC) service will isolate network access to a limited Internet only Guest Zone.
- Network access to all CWBFG systems will be based upon the principles of 'need to know' and 'least privilege'.
- Direct inbound network access from the Internet to any internal CWBFG critical business system is prohibited, unless a risk exception has been approved by the Information Security Office.
  - Use of intermediate systems (e.g. gateways, proxies, load balancers) must be used to protect these internal systems from external attacks.
- Areas containing network technology resources such as data centers, network switch closets, and other rooms containing equipment supporting computing infrastructure must be locked and access restricted to only those support personnel requiring access to perform their job responsibilities.
  - External support vendors requiring access to data center systems must be authorized.
  - Access records must be maintained for auditing and incident response purposes.
- Network services such as DNS, and DHCP, must not be configured to replicate CWBFG official network services, unless authorized by VP of Information Services and the Chief Information Security Officer.
- Bridging, routing or otherwise connecting the CWBFG network to other non-CWBFG networks without approval, is prohibited.
- All network access activity must be logged, including NetFlow and log data which captures at a minimum event source, date, user, timestamp, source addresses, and destination addresses. Logs must be forwarded to the Security Information Event Management (SIEM) for log correlation and analysis.

- Information Services are accountable and responsible for:
  - establishing and maintaining the approved network access methods, including:
    - managing all CWBFG network and network services, and any network connections with external third parties (e.g. Supplier or Cloud Service Providers);
    - restricting access to CWBFG network and network services to only authorized individuals in support of the CWBFG's business;
    - maintaining baseline configurations for network access methods;
    - staying current with the threat landscape, identifying new risks and addressing or remediating vulnerabilities associated with network services;
    - actively participating in on-going vulnerability and penetration testing, the Information Security Office will run to validate the network services implementation; and
    - remediating in a reasonable amount of time all high and medium risk findings from vulnerability and penetration tests that are run on a regular basis.
  - securing out-of-band channels used in the delivery or transmission for the purpose of:
    - managing non-Windows OS devices (e.g. storage, firewalls); and
    - limiting access for third party service provider TELUS using Remote One to manage network gear in the DMZ.
  - consulting with the Information Security Office and the Architecture Technical Review Board (TRB) on any new network access method, including:
    - requesting the Information Security Office to perform a risk assessment, vulnerability scan and penetration test of all new remote network access method;
    - remediating any high or medium risk findings from the risk assessment, vulnerability scan, or penetration testing findings, prior to implementation. If remediation is not possible, processing a risk exception with the Information Security Office; and
    - seeking the approval for any new network access method from the Architecture Review Board;
- The Information Security Office is responsible for:
  - providing security advice to Information Services personnel regarding the provisioning or changes to network access methods and/or security zones. This includes:
    - completing a risk assessment, vulnerability scan and penetration test for both new and existing approved network access methods to ensure they are and continue to remain secure;
    - ensuring all identified high and medium risks are remediated prior to implementation; and
    - facilitating the risk exception process for any non-standard network access methods.
  - maintaining the Information Security Architecture document in order to capture changes or the addition of any approved network access methods and/or security zones; and
  - maintaining this standard.

Security Zones

CWBFG requires groups of information services, users and information systems to be segregated within CWBFG networks into trust domains referred to as Security Zones.

Zones define the network boundaries and their associated perimeter defence requirements; providing protective measures to contain failures and reduce threats to availability of critical services. Increased zone granularity will reduce the attack surface and improve CWBFG's security posture.

General Requirements

- CWBFG must establish and maintain Security Zones to reduce risk of unauthorized access to its network, systems, applications, and information.
  - See *Appendix B* for the list of existing Security Zones that should be referenced when determining the placement of any new systems and/or services.
- The ***Information Security Classification Standard*** can be leveraged when determining the sensitivity of information and information systems, and their classification and/or categorization.
- Security zones group together entities (technology assets and users) with similar security requirements and levels of risk. ***Figure 1*** below provides a flowchart that can be leveraged when determining the appropriate zone:
  - All technology assets must be placed in a zone based on its classification, categorization, and overall risk profile.
  - The zone a user can access the CWBFG network is based on the user's role (e.g. employee/contractor, customer, or third party).

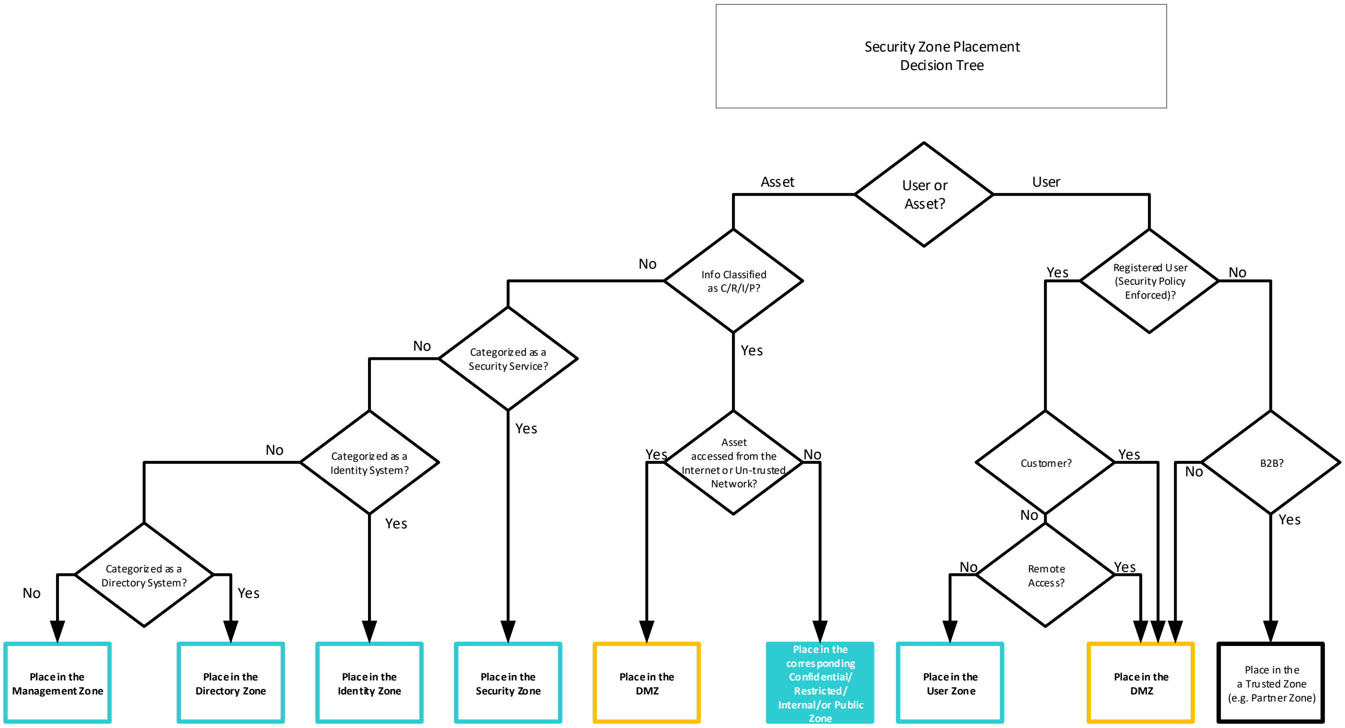
Security Zone Placement
Decision Tree
User or Asset?
Asset
User
Info Classified as C/R/I/P?
No
Yes
Registered User (Security Policy Enforced)?
Yes
No
Categorized as a Security Service?
No
Yes
Asset accessed from the Internet or Un-trusted Network?
Yes
No
Categorized as a Identity System?
No
Yes
Customer?
Yes
No
B2B?
No
Yes
Categorized as a Directory System?
No
Yes
Remote Access?
No
Yes
Place in the Management Zone
Place in the Directory Zone
Place in the Identity Zone
Place in the Security Zone
Place in the DMZ
Place in the corresponding Confidential/ Restricted/ Internal/or Public Zone
Place in the User Zone
Place in the DMZ
Place in the a Trusted Zone (e.g. Partner Zone)

Figure 1: Security Zone Placement Flowchart

- All systems within a given zone should be further grouped into sub-zones based on:
  - the services these assets provide, line of business, who/what access them, from/to where (i.e. type of zone) and their business criticality;
  - who owns, operates or manages these assets (e.g. creation of one or more sub-zone for third parties);
  - their inability to meet vulnerability management or patching requirements (e.g. an operating systems no longer supported by the vendor but required for business operations); and
  - Systems or configurations regarded as high risk by the Information Security Office after a full risk review.

- When a security zone is created and communication is required to traverse into another zone, a firewall must be used to restrict the flow of information to and from those zones.
  - Technology assets must not be interconnected simultaneously with different zones, sub-zones or external networks using multiple logical or physical network interface cards (also referred as multi-homing) with the exception of firewall and switches facilitating inter-zones connectivity.

- Zone separation is broken out into physical and logical categories and are defined as follows.
  - Logical Separation – separation utilizing software means such as VLAN, Mutliprotocol Label Switching (MPLS) Virtual Routing and Forwarding (VRF), zoning/tagging, etc. to logically separate inner zone traffic.
  - Physical Separation – separation utilizing hardware means such as firewalls primarily utilized to separate major zones. NOTE: The use of virtual firewalls while technically logical should be considered physical separation.
  - The following considerations will be followed when zoning.
    - Logical separation, such as network VLANs, by itself is not considered appropriate as a perimeter protection and therefore firewalls must be considered in addition to logical separations means.
    - Separation may be physical (OSI layer 1, hardware) or logical (OSI layer 2, virtualization in software); and
    - Virtualization technology (virtual machines, virtual LAN segments, etc.) may be utilized to logically separate traffic inner zone. However, traffic crossing to other major zones will require use of a perimeter/policy enforcement point.
  - To preserve security zone trust levels, the physical and logical separation approach shall be as follows:
    - Physical zone separation is required between the following zones.
      - Public to DMZ;
      - DMZ to all internal zones;
      - User Zone to Web/App: (Preferred Design: User → Load balancer → App/Web → Database)
      - App/Server to Database; and
      - Security, Identity, Directory, and Management zones to any internal zone or DMZ.

- Information Services (IS) is accountable and responsible for:
  - implementing and maintaining network subnets as per this standard;
  - ensuring the placement of technology assets into the correct security zone, with input from the Information Security Office;
  - decommissioning technology assets from security zones, when they are no longer required; and
  - documenting any risk exceptions for any technology asset which cannot be placed in the correct security zone.

- Information Security Office is responsible for:
  - providing consultation and assessing requirements, recommending security zones, and compensating security controls for proposed solutions during the solution design phase;
  - verifying technology assets have been placed in the correct security zone; and
  - facilitating the approval for any documented risk exception.

Remote Network Access

Remote network access enhances productivity by providing both CWBFG's authorized individuals with the flexibility and opportunity to conduct business and to stay in contact while away from the office. In the event of emergencies, remote access allows these system users to communicate with each other, access business applications, and business information from an alternate workplace.

General Requirements

- CWBFG provides remote access to CWBFG technology assets for business purposes only. All remote access is routed through the following approved managed network access control points: (AC-17 (3))

Remote Network Access Use Cases	Approved Remote Access Method
CWBFG Employees & Contractors on CWBFG managed endpoint devices.	• GlobalProtect – Client to Site VPN (Corporate Portal – vpn.cwbankgroup.com) • Virtual Desktop Infrastructure (VDI) • Citrix Gateway
CWBFG branch and remote office locations	• Multiprotocol Label Switching (MPLS) – IPSec DMVPN Tunnel between Branch ISR and Data Center edge router
Business Partners users on non-CWBFG managed endpoints	• Centrify Privileged Access Management (PAM) • GlobalProtect VPN (BYOD Portal – connect.cwbankgroup.com) • Citrix Gateway
CWBFG Azure	• Azure ExpressRoute (primary) – virtual private network • Site to Site VPN – IPSec (secondary)
For emergency vendor support – and approved exceptions	• Controlled by CWBFG staff • Approved by Information Owner and/or Information Custodian • MS Teams (Primary) • WebEx, GotoMeeting (except Zoom meetings)
Third Party – Approved Business Partners (B2B) transactions	• Site to Site VPN – IPSec • Dedicated physical network circuits • HTTPS (TLS1.2 or higher) with IP Whitelisting

- Information owners and/or Information Custodians are accountable and responsible for:
  - ensuring all remote access mechanisms used are secured, monitored, and restricted to only those systems or users with approved access. Enforced controls include:
    - using cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. (e.g. Virtual Private Networks - IPSec or Web Services – TLS) (AC-17 (2));
    - using multi-factor authentication mechanisms to strongly authenticate those remotely accessing the network from un-trusted networks;

    - verifying endpoints remotely entering the internal CWBFG network to ensure the minimum baseline configuration is in place (i.e. level of operating system and release level, use of anti-malware, personal firewall);
    - ensuring no new remote access requests are from any high risk countries deemed to be malicious by the Government of Canada's Canadian Center for Cyber Security (CCCS), more information can be obtained by visiting www.cyber.gc.ca;
    - seeking approval for any new remote access method into CWBFG network, including:
        - consulting with the Architecture Technical Review Board (TRB) and the Information Security Office to confirm security controls are sufficient;
        - requesting a risk assessment be performed for any new remote access methods. This may include performing a vulnerability scan or penetration test(s);
        - remediating any risk assessment, vulnerability scan or penetration tests prior to implementation into production.
    - re-authenticating sessions after 30 minutes of inactivity for all external non-CWBFG devices.
    - terminating all remote access sessions on CWBFG managed devices after 12 hours (e.g. 12 hours for Global Protect); and
    - preventing split tunneling or dual homing of remote endpoint devices. Remote access solutions must prohibit the use of split tunneling except for approved security policy exceptions.

- The Information Security Office is responsible for:
    - performing risk assessments, vulnerability scans and penetration testing prior to any non-standard remote access method being authorized for use. This includes facilitating remediation of any high or medium risks; and
    - monitoring remote access sessions to detect the potential of malicious attacks and to ensure ongoing compliance with remote access requirements (AC-17 (1)).

Third Party Network Access

CWBFG must limit Third Parties (typically vendor support personnel or business partners) remote access to only the assets needed to fulfill their obligations (AC-17).

General Requirements

- All Third Parties must:
    - use CWBFG approved remote access methods to provide the contracted Services. Enforced controls include:
        - Centrify Privileged Access Management (PAM) solution;
        - the usage of this network connection for any purpose other than delivering the contracted service is strictly prohibited; and
        - unauthorized remote access tools (e.g. Teamviewer, Bomgar, LogMeIn, etc.) are not allowed, unless they have been approved for use by the Information Security Office.
    - use CWBFG approved multi-factor authentication (MFA) methods to authenticate each individual accessing the CWBFG network;

  - agree and sign-off on CWBFG's ***Vendor/Third Party Information Security Requirements*** to be included in the contract/agreement. These agreements should include the relevant terms and conditions including, but not limited to, acceptable use, non-disclosure, and remote access policies, etc.

- Information Owner and/or Information Custodians are accountable and responsible for:
  - ensuring third parties are using approved CWBFG remote access and multi-factor authentication methods. If non-standard remote access methods are to be used:
    - a risk assessment must be completed including vulnerability scans and penetration testing;
    - all high and medium risks identified from risk assessment, vulnerability scans and penetration testing, must be remediated or a risk exception processed.
  - identifying, documenting, and maintaining remote access accounts and asset inventories; and
  - performing remote access reviews according to the ***Identity and Access Management Standard***, to aid in the regular validation and the removal of third party connections no longer required.

- The Information Security Office is responsible for:
  - performing risk assessments on any new remote access methods that allow third party access to CWBFG technology assets. This may include:
    - performing vulnerability assessments and penetration tests(s), prior to implementation.
    - ensuring all high and medium risk findings are remediated or a risk exception is processed, prior to implementation into production environments.

Wireless Access

CWBFG requires all wireless access to the CWBFG's network to be controlled using approved wireless access methods.

A Wireless Local Area Network (WLAN) enables access to CWBFG technology assets for devices without being physically wired to the network, but rather connected to CWBFG's 802.11 wireless network. This section address wireless access restrictions, configuration and connection requirements, and implementation guidance.

General Requirements

- Only approved CWBFG wireless access methods are allowed, and include:

Wireless Network	Access Method
CWB_Guest: non-CWBFG managed endpoints used by guests to access the Internet (e.g. vendors requiring access to the Internet to demo products or access their systems remotely).	• All Wireless access requests are initially processed through the Aruba Instant Access Point (IAP-305/315/515). Aruba's ClearPass solution delivers Radius server function and 802.1X authentication management. • All non-CWBFG managed devices are asked to register and only have access to the Internet.
CWB_Corporate: CWBFG managed endpoints used by employees, contractors.	• Based on the presence of user certificates and computer certificates, authorized laptops and Microsoft Surfaces are joined to the Corporate Internal Wi-Fi Zone and have access to internal resources and the Internet. • Authentication is through WPA2-Enterprise 802.1x EAP –TLS, computer certificate and User certificate. Advanced Encryption Standard (AES) to encrypt wireless data in transit.

- All wireless access mechanisms must be secured, monitored, restricted to only those with approved access. Enforced controls must include:
  - leveraging Advanced Encryption Standard (AES) to encrypt wireless data in transit.
  - enabling authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual, multi-factor authentication. (AC-17)
  - disabling wireless peripheral access of devices (such as Bluetooth and Near Field Communication (NFC)), unless such access is required for a business purpose and approved by End User Computing. Without strong cryptographic authentication checks, malicious third parties can use Bluetooth to connect to a device they shouldn't have access to, or trick targets into thinking their rogue device is a trusted one.
    - Any CWBFG provided devices such as Bluetooth keyboard and mouse peripherals must use the maximum level of security the product can support. Switch off your Bluetooth when not in use will neutralize most security concerns. Others requirements include:
      - Rejecting pairing requests from unknown devices.
      - Keeping your firmware updated at all times.
      - Buy a device that has sufficient security features.
    - Use of Near Field Communication(NFC) must take into consideration the following requirements:
      - Users should not tap any tags that aren't somehow physically protected, perhaps behind glass or plastic; those that swing freely in public places are much more likely to be tampered with. When a tag is tapped, carefully watch the device to see what actions the tag prompts. Often, there are suspicious, tell-tale prompts that appear (much like aggravating pop-up browser screens on your computer) serving as warnings that something is awry.
      - Users should not bump phones to exchange information with other individuals that are not considered trusted. A smart threat actor can potentially use this opportunity to transfer spyware to the device.
      - Developers must add password protection and encryption to their products and applications. Consult the NFC World if new business initiatives plan to use NFC to serve CWBFG customers for the latest security concerns.
  - utilizing Simple Network Management Protocol (SNMPv3) agents which includes mechanisms to provide strong security for network management of access points and clients.
  - physically protecting wireless access points to protect them from physical theft or tampering (i.e. access to the 'reset' button, LAN or power cables, etc.);
  - logically separating wireless access points with different security profiles into different security zones and separating wireless networks from wired networks, using filters, firewalls, or proxies;
  - detecting, blocking and reporting of unauthorized wireless access points using a network access control service;
  - logging network activities to facilitate incident response investigations.
- Information Services (IS) is accountable and responsible for:
  - the management of CWBFG wireless networks, and configuring them in a secure manner;
  - reviewing the wireless configuration on an annual basis to ensure security settings are enabled;
  - reviewing and facilitating any new requests for wireless networks, to ensure the new configuration complies with this standard;
  - deploying and applying firmware and software upgrades, fix packs, and patches for managed wireless services; and
  - documenting the operational processes followed for maintaining access methods to approved wireless networks.

- The Information Security Office is responsible for:
  - advising Information Services on the mandatory wireless requirements;
  - performing compliance reviews and/or risk assessments on any new wireless networks, or ones undergoing major enhancements or upgrades; and
  - tracking the progress of Wi-Fi industry standards, features, threats, and vulnerabilities. This helps to ensure the continued secure implementation of WLAN technology. The latest information regarding Wi-Fi can be obtained by visiting www.wi-fi.org.

Mobile Device Access

CWBFG requires a Mobile Device Management ("MDM") service to secure, monitor, and manage corporate mobile devices. This service provides software distribution, policy management, inventory management, security management, and service management for corporate mobiles devices.

Microsoft Intune is CWBFG's approved MDM solution for controlling mobile devices used by CWBFG employees and providing secure access to technology assets.

Principles Governing Corporate Owned Mobile Devices

- The requirements to access CWBFG information assets on a corporate owned mobile device, includes:
  - mandatory mobile device enrollment in CWBFG Intune MDM through managed applications.
  - following the Apple Device Enrollment Program (DEP) process for corporate owned iPhone; and
  - leveraging approved data storage services such as ShareFile, and when available OneDrive or SharePoint Online to store CWBFG information.

MDM Enrolled User Responsibilities

- To protect information assets, mobile device users are required to:
  - enroll in the MDM: All users must ensure their mobile device is enrolled in CWBFG's MDM system.
  - accept the MDM Terms and Conditions: All users must accept the MDM Terms and Conditions or the enrollment with MDM will not proceed, which include CWBFG's right to:
    - monitor access and/or connection to CWBFG assets, to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity. This assists in identifying devices that may have been compromised by external parties; and
    - access the mobile device to enforce security controls as outlined within this standard.
  - refrain from loaning a CWBFG provided mobile device to unauthorized individuals;
  - avoid connecting their mobile device to unsecured Wi-Fi networks;
  - maintain the current versions of device Operating System (OS) software;
  - prevent the backup of CWBFG data to cloud based on-line storage services which have not been approved;
  - enable Touch ID (if available), passcode and inactivity timeouts to protect the contents of the device;
  - comply with the Acceptable Use Policy;
  - avoid scanning Quick Response (QR) codes from untrusted sources, as these may direct the user to malicious websites;
  - comply with the following business travel requirements to:
    - secure all mobile devices from physical theft;

    - where possible, refrain from storing CWBFG and other confidential information (e.g. Personally Identifiable Information) on the device. The authoritative source of information should be maintained on CWBFG systems;
    - keep all mobile device passwords confidential (except in those rare occasions when Customs or Border Agents legally request it). If the password has been disclosed intentionally or otherwise, then it must be changed immediately; and
    - avoid connecting devices to untrusted charging device/station(s), like those found at airport kiosks. Connecting a mobile device using a USB cable can allow software running on another device to interact with the device in an unexpected way. As a result, a malicious computer could gain access to sensitive data or install malware.
  - abide by the baseline Mobile Device Configuration: The MDM Compliance Policy checks mobile devices for the following basic configuration:
    - requires password settings on mobile devices;
    - requires a complex password, and expects a minimum password length of 8 characters;
    - requires a password expiry of 90 days;
    - requires an inactivity timeout of 2 minute; and
    - tests to see if mobile device is jailbroken or rooted.
  - remediate any mobile device non-compliance issues: If the corporate mobile device configuration changes, the device may be marked as non-compliant. It will be the user's responsibility to modify their device settings in order to re-establish device compliance and access to CWBFG information.
  - avoid the use of screenshot features: Users must not use screenshot CWBFG applications/features to capture information.
  - report if their device is not functioning properly to the Help Desk. Malfunctioning devices could indicate a security risk and should be investigated immediately;
  - report all lost, stolen, compromised corporate mobile devices immediately to the CWBFG Help Desk. Depending on the incident, the MDM administrator may take the following actions:
    - block access from the device;
    - perform a selected device wipe by deleting just the CWBFG data;
    - perform a full device wipe, if required. This action deletes all CWBFG and personal data on device. If there are no previous backups of personal data performed by the user, it will be lost. Since it is a CWBFG owned device and due to safeguarding information assets, an MDM administrator will not require consent from the user to perform this device wipe action; or
    - locate a lost Corporate Mobile device.

CWBFG Information Assets Protection

Removal of information assets from MDM enrolled Mobile Devices

- CWBFG reserves the right to remove information assets or access to data on all MDM enrolled mobile devices, as required.
- The following conditions constitutes the removal of CWBFG information assets from corporate owned mobile devices, if:
  - the user is no longer employee or under contract with CWBFG;
  - the mobile device is lost or stolen;
  - the mobile device is offline for an extended period of time; or
  - the mobile device is deemed to be compromised or deemed to pose a threat to CWBFG.

Blocking and Monitoring Mobile Device Access

- To protect CWBFG information assets, MDM administrators may block:
  - mobile applications that are deemed to be a threat to the CWBFG organization;
  - mobile devices from accessing CWBFG data should the device be reported as lost, stolen or in violation of policy; or
  - mobile devices from accessing CWBFG data from high risk networks and countries as guided by CWBFG Information Security Office.

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. • Accountable to have and maintain written standards and procedures necessary to ensure implementation of and compliance to this standard. • 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. • Responsible to have and maintain written standards and procedures necessary to ensure implementation of and compliance to this standard. • Responsible to provide support and guidance to assist employees to fulfill their responsibilities of complying with this standard. • Consulting with Sr. Manager, Security Governance, Risk and Compliance and Sr. Manager, Security Operations, as required.
CWB's Executive Leadership Team, Senior Leadership Team, Directors, and Managers	• Understand and comply with this standard and supporting policy in its entirety. • Responsible to create and maintain processes and procedures to support this standard and supporting policy. • Responsible to ensure that all appropriate personnel are aware of and comply with this this standard and supporting policy. • 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.
CWB employees, contractors, third-party service provider, etc.	• Understand and comply with this standard and supporting policy in its entirety. • Implement this standard with supporting processes and procedures. • Report vulnerabilities and breaches.

Appendix A – Document Control

Document Status

Document Name	Network Access 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	Vikram Singh	Joanne Pearson	Document creation
Draft 0.2	Joanne Pearson	Vikram Singh	Updated based on initial review
Draft 1.0	Vikram Singh	Joanne Pearson	Prepare Standard for review
Draft 2.0	Joanne Pearson	Thomas Matthews	Updates made incorporating Thomas Matthews feedback. Ready the standard for CISO review.
Final 1.0	Joanne Pearson	Cory Gould	Feedback incorporated and published in Keylight

Appendix B – CWBFG Security Zones

The following Security Zones have been implemented in the CWBFG On-Premise network and CWBFG Azure Network. These zones and their descriptions can be referenced along with the placement decision flowchart in ***Figure 1***, when determining the placement of new systems or services.

Zone Name	Purpose	Network Access Requirements
Public Zone Uncontrolled	Comprised of external non-CWBFG systems, services not 100% controlled by CWBFG Information Security policies and standards. • *CWBFG Office 365 Zone:* Comprised of CWBFG Office 365 services, including email, Sharepoint, etc. services. • *CWBFG Azure Zones*: Comprised of CWBFG Azure subscriptions hosting systems and services that have been migrated from CWBFG on premise Data Centers. • *CWBFG SaaS Zone:* Comprised of SaaS cloud based services used by CWBFG. • *Public Internet Zone:* Comprised of systems accessing CWBFG internal network via the Internet.	This zone represents all networks outside of the CWBFG on-premise network, and network connectivity is primarily established over an un-trusted network. • For CWBFG Office 365 services, there is a level of trust that systems and services provided are secure, confirm by independent third party attestations (e.g. SSAE 16 SOC 2 Type 2 and ISO27001 certification). – Users can directly access this network from any network – Direct administrator access to these services must be restricted to a limited number of privileged accounts responsible for providing support. • For CWBFG Azure services, there is a level of trust that systems and services are secure, network access if restricted, and security zones mirror CWBFG on-premise zoning model. – Users indirectly access applications through load balancer/proxies from the internal CWBFG network. – Direct administrator access to this network must be restricted to a limited number of privileged accounts responsible for providing support. • For CWBFG contracted SaaS services, agreements contain the security requirements when CWBFG information is stored, used, processed. Most SaaS have independent third party attestations (e.g. SSAE 16 SOC2 Type 2 and ISO 27001 certification. – Users can directly access this network from any network (internal and Internet). – Direct administrator access to these services must be restricted to a limited number of privileged accounts responsible for providing support. • For access from the Internet – Most systems accessing CWBFG internal systems are deemed un-trusted, and CWBFG's policies and standards may not apply, and – Users can directly access this network from the internal User Zone.

Zone Name	Purpose	Network Access Requirements
Enterprise Edge Perimeter (DMZ) Controlled	• *Public Access Zones VLAN 111, 112, 113, & 114*: All external communications (i.e. corporate or third party) should be terminated in the DMZ(s) either through proxy or terminal services technologies. The DMZs zones must not host critical business services. Those services must operate within the internal zone(s). • Public VLAN 111 – Citrix Sharefile Server – External SMTP – LDAP/LDAPs • Confidential VLAN 112 – T24 DMZ Interface – Maximum Transporter servers – AD LDAP vServer • Internal VLAN 113: – VDI • Restricted VLAN 114 – NPS vServer MFA Radius – LDAP/Radius – SFTP – Citrix Gateway • *Guest Wireless Zone* (VLAN 800) Comprised of wireless access points which integrate with internal Wi-Fi management systems that allow Guest access to the Internet or users on managed CWBFG devices inbound corporate network access.	This DMZ zone is meant to create a physical barrier between the CWBFG internal network and the Public Zone. All communications entering or leaving the CWBFG internal network should go through the appropriate DMZ(s). Public Access Zone - Systems that can be placed in this zone include: • Proxy systems, which handle inbound and outbound requests (via Load Balancers) on behalf of users and systems. • Remote access gateways (VPN, Citrix) for business users and virtual desktop infrastructure remote access for support staff. Network Access: • Users cannot directly access this zone from the internal network • Direct access to this zone must be restricted to a limited number of privileged accounts responsible for providing support. Guest Wi-Fi Zone: Wireless access control points integrated with internal Wi-Fi systems, together determine the level of wireless access allowed depending upon on what type of device (managed or unmanaged) used. • Guest systems can directly access this zone directly and can only access the Internet. • Corporate system can directly access this zone and are redirected to the internal Corporate Wi-Fi zone which has access to the internal systems and services that have been authorized. • Direct administrator access to these systems must be restricted to a limited number of privileged accounts responsible for providing support.

Zone Name	Purpose	Network Access Requirements
CWBFG Branches (MPLS) Controlled	Comprised of CWBFG systems that are placed in each Branch office network. Systems are joined to the CWBFG on-premise network and other trusted cloud based services. Some branch network have direct access to the Internet. Some branch networks have established their own wireless network.	• Local users have direct access to the Branch network, including the wireless network. • Direct administrator access to systems in this zone must be restricted to a limited number of privileged accounts responsible for providing support.
External Network Perimeter Partners Zone External Controlled	Comprises of Business Partner systems that integrate with CWBFG internal systems (e.g. Central 1, Everlink, etc.)	• Trusted partner systems that are permanently connected to CWBFG systems. • Direct access to this zone must be restricted to a limited number of privileged accounts responsible for providing support.
Partner Services (VLAN 158) B2B/B2P Access Zone Controlled	Comprised of systems that require business to business and/or business to partner transmissions, such as: • Secure File Transfer • Transmissions to/from partner systems • Gateway services	• Systems that integrate with business and partner systems primarily used to transmit or received data in a secured fashion. • Direct access to this zone must be restricted to a limited number of accounts responsible for providing support or those requiring access to the SFTP and Transmission services.
Internal DMZ PROD -VLN 133 & Non-Prod VLAN 142	Comprised of systems (e.g. Load Balancer, VDI, Felix Portal) that help with controlling access and the flow of information to/from internal systems	• Direct access to this zone must be restricted to a limited number of privileged accounts responsible for providing support.
Core Network Internal Services Zones *CWBFG Azure: Hub Zones*	Comprised of multiple virtual local area network (VLAN) segments that constitute logical security zones, including: • *Security Zone - VLAN 184:* comprised of systems that provide core security related services. • *Identity Zone – VLAN 157*: comprised of systems that provide core Identity related	Security Zone: Direct access to this zone must be restricted to a limited number of privileged accounts responsible for providing support. Identity Zone: Direct access to this zone must be restricted to a limited number of privileged accounts responsible for providing support.

Zone Name	Purpose	Network Access Requirements
	services using in providing secure access to CWBFG systems and information. • *Directory Zone – VLAN 128*: zone where most of the legacy common IT services were deployed. It also includes some banking application and database servers (e.g. Wave, Maximizer, etc.) • *Internal DMZ – VLAN 133*: Comprised of Internal Load Balancers nodes that gates data flows into/out of application zones. • *Management Zones – VLAN 132, 125, 141*: Comprised of management consoles and tools to help manage IT and core security services. • *HSM Zone* – VLAN 129: Comprised of Hardware Security Module (HSM) system used to provision cryptographic keys for critical functions such as encryption, and authentication.	Directory Zone: Direct access to this zone must be restricted to a limited number of privileged accounts responsible for providing support. Once authenticated, application users can access application servers via the load balancers. Internal DMZ: Direct access to this zone must be restricted to a limited number of privileged accounts responsible for providing support. Management Zones: Direct access to these zones must be restricted to a limited number of privileged accounts responsible for providing support. HSM Zone: Direct access to these zones must be restricted to a limited number of privileged accounts responsible for providing support.
User Zones	• *User Zone – VLAN 64*: Comprised of systems that represent endpoint client devices (such as laptops, desktops, mobile, IP phones, printers, etc.). • *PAW Zone* – VLAN 82: Comprised of privileged access workstations.	User Zone: • Users when signed on to their workstations have access to this zones. • Systems here may connect to the Internet/Public Zone for legitimate business purposes. PAW Zone: Direct access to these zones must be restricted to a limited number of privileged accounts responsible for providing support.

Zone Name	Purpose	Network Access Requirements
Corporate Wireless Zone – VLAN 400	Comprised of wireless systems that provide wireless access for CWBFG managed devices.	• Guest systems cannot access this zone. • Corporate system can directly access this zone and have access to the internal systems and services that have been authorized. • Direct administrator access to these systems must be restricted to a limited number of privileged accounts responsible for providing support.
Confidential, Restricted, Public, Internal Application and Database Zones CWBFG Azure – Production Zone	Comprised of Servers that separate application servers from and database servers. • Confidential – Application Zone: VLAN 147; Database Zone: VLAN 146 • Confidential – T24 Zone: Browser, Application and DB Zone: VLAN 129 • Confidential – SAS/EDW Application Zone: VLAN 154 • Confidential – Mable DB Zone: VLAN 170 • MuleSoft Zone: VLAN • Restricted – Application/Web Servers – VLAN 160 • Restricted – Database Servers – VLAN 161 • Internal – Application/Web Servers – VLAN 164 • Internal – Database Servers – VLAN 165 • Public – Application/Web Servers – VLAN 166 • Public – Database Servers – VLAN 167	• Users can access application servers via Load Balancer proxy. • Direct access to these zones must be restricted to a limited number of privileged accounts responsible for providing support.
Directory VLAN 128 Application & DB	Along with core IT services, this VLAN also contains application and database servers for: • Wave • CSM • Maximizer • MacLeans & Partners • SQL DB servers	• Users can access application servers via Load Balancer proxy. • Direct access to these zones must be restricted to a limited number of privileged accounts responsible for providing support.

Appendix C – Definitions

The following table highlight key definitions used in this Standard.

CISO	Chief Information Security Officer
CWBFG	Canadian Western Bank Financial Group
Mobile Device	A portable computing device that (1) has a small form factor so it can easily be carried by a single individual; (2) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (3) possesses local, nonremovable or removable data storage; and (4) includes a self-contained power source. Mobile devices may also include voice communication capabilities, onboard sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples are smartphones and tablets.
Network Access	Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).
Remote Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
Security Zone	Security zones are established through network segmentation which is the act or practice of splitting a computer network into subnetworks, each being a network segment or security zone, where technology assets with the same trust or risk profile are grouped together and are placed to ensure each zone is given the appropriate level of protection based the assets' profile. When a threat actor gains unauthorized access to a network, segmentation or "zoning" can provide effective controls to limit further movement across the network. Segregation is typically achieved by a combination of firewalls and VLANs (Virtual Local Area Networks). Software-Defined Networking (SDN) can allow the creation and management of micro-segmented networks.
Virtual Private Network (VPN)	An approach to providing authentication and secure data communications. VPN (Virtual Private Network) technology creates an encrypted layer of networking on top of another network, including a wireless network.
Wireless Access Point (WAP)	The term access point includes special-purpose hardware as well as general-purpose computers that are configured to act as base stations or transceivers for wireless LANs.