1.0 INTRODUCTION

As and where applicable, all units, specified devices, communications and systems integration, must meet all industry best practices and standards. RF transmitting devices, where not permissible, must be supplemented with devices that have limited, or no wireless communication protocols. All device recommendations/replacements/data hosting environments must be approved prior to integration.

2.0 ON-SITE WORKSTATIONS

2.1 Workstations located on-site must have a backup available off-site and available rapidly in case of failure.

2.2 Workstations software, including the Operating System, must be patched and updated regularly as recommended by the software provider.

2.3 All USB ports on workstations must be disabled.

3.0 OT NETWORK DEVICE MANAGEMENT

3.1 OT devices must be carefully selected from reputable vendors, use standardized models, and be configured in a secure manner to ensure the reliability and security of the OT network. OT Network devices at client sites may not be installed on OT Networks by any individual or group unless approved by BGIS.

3.2 OT Network devices must be patched or updated in response to security vulnerabilities and with the latest supported code as soon as possible and within 30 days of release.

3.3 OT Network device configurations or changes must be documented, reviewed, tested, and deployed in accordance with an IT change management policy.

3.4 OT Network and network device documentation must be classified, stored, and handled in accordance with industry best practices and standards.

3.5 All OT network documentation containing specific network configuration and networking addressing information must be classified as “Confidential” and must not be shared with any party other than BGIS without BGIS’s written consent.

3.6 OT networks must be available for independent assessment by internal/ external assessors/ auditors.

4.0 OT NETWORK DEVICE CONFIGURATION

4.1 OT Network devices must be on a dedicated hardware device platform with only essential network operations software or service installed and running on them.

4.2 Where applicable, OT network devices must be built to provide high availability and disaster recovery capabilities to meet established network and business service level requirements.

4.3 OT Network devices must not share computer resources with other applications or services, except for enabling security controls such as security monitoring and analysis.

4.4 OT Network devices must support traffic and security monitoring tools that meets industry best practices such as Zabbix or other tools pre-approved by BGIS

4.5 OT Network device default passwords must be changed before installation and deployment. Password must be at least 30 characters long and include at least (1) upper case letter, (1) lower case, (1) number, and (1) special character.

4.6 OT Network devices must maintain their configuration and security settings and access controls during a reset or reboot process, or when a network device fails over to a backup network device.

4.7 OT Network firewall devices must be configured to identify security incidents and to allow incident response procedures to be initiated. BGIS must be notified of any instance of a security event related to OT Network devices.

4.8 OT Network device configuration information must be securely erased before decommissioning and disposal.
4.9 OT Network devices should be hardened to ensure local physical access requires authentication (example: ensure console connection requires a password and disabling any auxiliary connections like USB).

5.0 ACCESS TO MANAGED OT NETWORK DEVICES

5.1 Access to OT network devices must be approved only for authorized personnel.
5.2 Access permissions and user accounts to OT network devices must be certified at least biannually and the verification artifacts are to be stored securely.
5.3 Access to OT network devices and network management systems must be immediately revoked when an administrator changes work responsibility. All service and network administrator passwords must also be reset.
5.4 Notwithstanding service and network administrator accounts, user accounts to OT network devices and network management systems must be specific individual user accounts with no generic or shared user accounts. Access to OT network devices and network management systems must be immediately revoked when an individual user account changes work responsibility.
5.5 Where possible, access to OT network devices to manage the device should use multifactor authentication.
5.6 Access to OT network devices and network management system using telnet, ftp, or other unencrypted protocols are prohibited.Create a separate account for all users. General accounts for OT device configuration access are prohibited.

6.0 OT NETWORK PERIMETER SECURITY

6.1 Where applicable, OT network devices must have Intelligent Document Processing (IDP) capabilities (or equivalent) and they must be enabled for all traffic flows,
6.2 OT network equipment installed at client sites must be available for independent assessment by BGIS.
6.3 The OT network perimeter must ensure all connectivity to/from the Internet travels through approved network gateways. The OT gateway should be the only gateway available between the local OT networks(s) and the untrusted zones.
6.4 The network perimeter must be configured to filter network traffic to and from the Internet including the following rules:
- 6.4.1 Implied Deny-all rule; All OT network traffic is dropped unless it is explicitly allowed.
- 6.4.2 All OT firewall rules must use the principle of least privilege (only allow what is needed for the application to work).
- 6.4.3 OT Firewall rules must be created as not to allow 3rd party apps to circumvent security principals (network segregation) or features. Example: outbound internet policy should ensure that remote control applications (example: TeamViewer) do not allow unauthorized remote connectivity back to the OT system.
- 6.4.4 All traffic traversing the OT network (intrazone or interzone) must be encrypted using a minimum of TLS 1.2 or IPSEC.

6.5 Remote access from the Internet or other external networks must be considered untrusted and must be authenticated at minimum by a known and confirmed source IP. This type of connectivity should only be used by application traffic. Remote access traffic must originate from Canada.
6.6 Multifactor authentication must be used when remotely connecting from an end user computer to the OT network.
- 6.6.1 Sources of traffic from Internet sites and IPs known to contain or originate attacks and malware or to support spam, malicious software, denial of service attacks, network attack platforms, offensive material, or other technology risks to client equipment and systems must be blocked.
- 6.6.2 OT Network internal networks must be segregated where applicable. (i.e. OT devices must not be on the same subnet as corporate users.

6.7 All user remote access through untrusted devices need to pass a Host Information Profile (HIP) check before being able to connect to the OT VPN. (Example: The user's computer must be using windows 11 with the latest windows patches).
- 6.7.1 Where applicable, OT networks should have a minimum layer 2 network access control (NAC)

7.0 WIRELESS NETWORK ACCESS

7.1 OT Networks often use basic authentication protocols like WEP or WPA. This is acceptable if these networks follow principal of least privilege and network segregation.
7.2 Wireless OT networks must be hidden.
7.3 Wireless OT networks must be dedicated to the functionality of the OT system. For example, Guest Wi-Fi users shall not have access to the OT wireless network.
7.4 Local user Wi-Fi networks must have user-level authentication (Example: RADIUS)

8.0 OT ADMINISTRATION

8.1 OT Networks shall have an assigned user that is responsible for approving and authorizing any requests related to the respective OT network. If an OT network does not have an assigned administrator, then an administrator must be assigned before any changes can be processed.
8.2 User access through the OT network should be fully authenticated (with 2 factor auth) and use a user repository that can be audited and reviewed.

9.0 CLOUD SERVICES

9.1 All cloud services must meet the following minimum requirements:
- 9.1.1 Data Residency in Canada.
- 9.1.2 All data to be destroyed (certification letter, signed by Authorized Company representative) at termination of contract after transfer to client preferred storage service
- 9.1.3 BGIS reserves the right to conduct a Security Vulnerability Assessment on any suggested cloud-based platforms identified for use. The assessment will require that the vendor provide the following information (but not limited to) prior to award or at any other time throughout the life of the contract:
  - a) EULA (end user license agreement)
  - b) Privacy Statements/Policies
  - c) Data Residency and Destruction Policies

10.0 BGIS FIREWALL REQUIREMENTS

10.1 Third party vendor OT systems and devices shall be connected via a vendor managed firewall as per the following architecture.