1.0 OT NETWORK DEVICE MANAGEMENT

1.1 Operational Technology (OT) Network devices must use a vendor, model and secure configuration.
1.2 OT Network devices may not be installed on OT Networks by any individual or group outside of administration team unless approved by the client.
1.3 OT Network devices must be patched or updated in response to security vulnerabilities when applicable.
1.4 OT Network device configurations or changes must be documented, reviewed, tested, and deployed in accordance with an IT change management policy.
1.5 OT Network and network device documentation must be classified, stored, and handled in accordance to regional government policies.
1.6 All OT network documentation containing specific network configuration and networking addressing information must be classified as “Confidential”.
1.7 OT networks must be available for independent assessment by internal/ external assessors/ auditors.

2.0 OT NETWORK DEVICE CONFIGURATION

2.1 OT Network devices must be on dedicated hardware device platform with only essential network operations software or service installed and running on them.
2.2 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.
2.3 OT Network devices must not share computer resources with other applications or services, except for enabling security controls such as security monitoring and analysis.
2.4 OT Network devices must support Zabbix or other IT approved tools for network traffic and security monitoring.
2.5 OT Network device default passwords must be changed before installation and deployment at the instruction of BGIS.
2.6 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.
2.7 OT Network devices must be configured to transmit security event data to the Security Information and Event Management (SIEM) System to enable the detection of security incidents and to allow incident response procedures to be initiated.
2.8 OT Network device configuration information must be securely erased before decommission and disposal.
2.9 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).

3.0 ACCESS TO MANAGED OT NETWORK DEVICES

3.1 Access to OT network devices must be approved only for authorized personnel.
3.2 Access permissions and user accounts to OT network devices must be certified at least biannually and the verification artifacts are to be stored securely.
3.3 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.
3.4 Access to OT network management segments for BGIS network devices must be on a separate secured network. Management access to OT network devices must not be permitted from an insecure network (e.g. from the Internet).
3.5 Where possible, access to OT network devices to manage the device should use multifactor authentication.
3.6 Access to OT network devices and network management system using telnet, ftp, or other unencrypted protocols are prohibited.

4.0 OT NETWORK PERIMETER SECURITY

4.1 Where applicable, OT network devices must have IDP capabilities and they must be enabled for all traffic flows, excluding sanctioned BGIS scanning type traffic.

4.2 OT network equipment must be available for independent assessment by Internal Audit.

4.3 The OT network perimeter must ensure all connectivity to/from the Internet or to any untrusted network from BGIS OT networks travels through approved network gateways. The OT gateway should be the only gateway available between the local OT networks(s) and the untrusted zones.

4.4 The network perimeter must be configured to filter network traffic to and from the Internet including the following rules:

4.5 Implied Deny-all rule; All OT network traffic is dropped unless it is explicitly allowed.

4.6 All OT firewall rules must use the principal of least privilege (only allow what is needed for the application to work).

4.7 OT Firewall rules must be created as not to allow 3rd party apps to circumvent security principals (network segregation) or features (remote access through BGIS OT VPN). Example: outbound internet policy should ensure that remote control applications (example: TeamViewer) do not allow unauthorized remote connectivity back to the OT system.

4.8 All traffic traversing the OT network (intrazone or interzone) must be encrypted. For encryption, TLS is accepted, and the minimum version of TLS is TLS 1.2. IPSEC is also accepted.

4.9 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.

4.10 Multifactor authentication must be used when remotely connecting from an end user computer to a BGIS OT network.

4.11 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 BGIS must be blocked.

4.12 OT Network internal networks must be segregated where applicable. (Example 1: OT devices must not be on the same subnet as corporate users. (Example 2: OT devices for building automation must not be on the same network as OT devices for the building leak detection system).

4.13 All user remote access through untrusted devices (non-BGIS machines) need to pass a Host Information Profile (HIP) check before being able to connect to the BGIS OT VPN. (Example: The user's computer must be using windows 10 with the latest windows patches).

4.14 Where applicable, OT networks should have a form of network access control (NAC) – either layer 2 or layer 3 NAC.

5.0 WIRELESS NETWORK ACCESS

5.1 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.

5.2 Wireless OT networks must be hidden when possible.

5.3 Wireless OT networks must be dedicated to the functionality of the OT system. For example, Guest Wi-Fi users should not share the OT wireless network.

5.4 Local user Wi-Fi networks must have user-level authentication (Example: RADIUS)

6.0 OT ADMINISTRATION

6.1 OT Networks should 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.

6.2 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.

7.0 CLOUD SERVICES

7.1 All cloud services must meet the following minimum requirements:

7.2 Certified ISO/IEC 27001 and compliant in ISO/IEC 27017, and ISO/IEC 27018 relating to cloud services.

7.3 Data Residency in Canada, the United States, United Kingdom or Australia.

7.4 All data to be destroyed (certification letter, signed by Authorized Company representative) at termination of contract after transfer to client preferred storage service

7.5 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:

7.6 EULA (end user license agreement)

7.7 Privacy Statements/Policies

7.8 Data Residency and Destruction Policies

7.9 ISO/IEC 27001certification

7.10 Demonstration of the Vendor's IT Security management Statement identifying compliance of ISO/IEC 27017/27018 during ISO/IEC27001 certification and/or independent evaluations of Compliance standards relating to ISO/IEC 27017/27018.

8.0 BGIS FIREWALL REQUIREMENTS

8.1 Third party vendor OT systems and devices will be connected via a BGIS managed firewall as per the following architecture. Vendor is to cooperate with BGIS OT network managers to make a secure connection via the firewall as per the following diagram.