Operational Security Requirements Check List

Physical Security Requirement (ISO 27001 Reference: A.11)

- Maintain the physical security of the operating environment
- Put in place appropriate procedures to ensure that the responsibilities for the maintenance of a secure operating environment are properly allocated and discharged
- Ensure that adequate procedures are in place for the physical protection of the service equipment. This must as a minimum cover:
  - Intruders
  - Fire
  - Water
  - Environmental (such as: storms)
  - Physical damage (accident)
  - Physical damage (deliberate)
- Implement physical and environmental controls to protect the service commensurate with the level of risk. The following minimum standards are to be implemented in any accommodation of the service equipment:
  - Equipment to be housed in unoccupied areas
  - Equipment area to be physically secured with controlled access
  - handheld fire extinguishers easily accessible
  - Automatic fire suppression equipment in place
  - Appropriate fire detection equipment installed
  - Smoke detection equipment installed
  - Water detection equipment as appropriate
  - Appropriate power supply cleanliness and contingency
  - Appropriate environmental controls
  - Appropriate regular cleaning regime
  - Cables properly managed
  - Cables properly labelled
  - Telephone with emergency numbers prominently displayed
  - Contingency plan initiation sequence prominently displayed
  - Location of backup media prominently displayed close to associated equipment

Destruction of time expired, faulty or failed media (ISO 27001 Reference: A.8.3)

- The Company must ensure that its staff understand the sensitivity associated with all media within the service and put in place appropriate procedures for its secure destruction in case of a fault, failure or life expiry

Secure system and network configurations (ISO 27001 Reference: A.13.1)

- The Company must ensure that all systems that make up the service are configured in accordance with a recognized standard for operating system security

Control of access to the systems and networks to limit the incidence of: (ISO 27001 Reference: A.9.2, A.13.1)

The Company must have control in place to limit, as a minimum, the following incidences:

- Unauthorized access to organization systems
- Interference with network components
- Performance degradation across the network
- Interference with network traffic

Logging and monitoring of events (ISO 27001 Reference: A.12.4)

The Company must consider having a process in place to, as a minimum, monitor and log the following:

- Legitimate access
- Authentication exceptions
- Authority exceptions
- Privilege changes
- Data object owner changes
- Export of information
- Out of hours access

Adequate documentation (ISO 27001 Reference: A.12.1.1)

- To enable proper delivery of the service, the provider must maintain, as the minimum, the following documentation:
  - CSOD Technology Overview

Appropriate management of personnel (ISO 27001 Reference: A.7)

The Company must have procedure in place to manage the following personnel issues relating to information risk management:

  - dismissal
  - resignation
  - termination
  - transfer
- Ensure staff and subcontractor have an understanding of information risk management threats and concerns relating to the outsourced arrangement and of relevant information risk management policies
- The Company’s Staff assigned to the outsourced arrangement must be made aware of the City's requirements, expectations related to the security and privacy of the data
- The Company’s Staff assigned to the outsourced arrangement must receive training and regular updates on relevant information risk management policies and procedures

Appropriate procedures for dealing with malicious software (ISO 27001 Reference: A.12.2)

- The Company must put in place appropriate checking and elimination procedures to ensure that the service is not affected by viruses during development, maintenance and operation

Notification and management of changes (ISO 27001 Reference: A.12.1.2)

- The Company must have procedure to notify the City of any changes that may affect the environment of the outsourcing arrangement
- The Company must have process for managing changes to the outsourcing arrangement
- The Company must have process for testing changes
- The Company must successfully test all changes before implementation

Management of test data (ISO 27001 Reference: A.14.3)

- The Company must demonstrate that its testing regime is able to adequately manage test data
- The Company shall not use City production data for testing purposes.
- If the use of production information is essential to the successful implementation of the service, the Company must have process to seek City's approval and implement adequate procedures to manage the data appropriately. Not withstand to the approval from the City, the Company must manage the data in compliant with the regulatory / legislative requirements.

Technical Vulnerability Management (ISO 27001 Reference: A.12.6)

- The Company must put in place appropriate checking and remediation procedures to prevent exploitation of technical vulnerabilities. The Company must ensure that information about technical vulnerabilities shall be obtained in a timely fashion and the City's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Key Management (ISO 27001 Reference: A.10.1.2)

- The Company must have policy and procedures on the use of cryptographic controls for protection of information, and also for the protection and lifetime (lifecycle management) of cryptographic keys.

Capacity Management (ISO 27001 Reference: A.12.1.3)

- The Company must ensure that the use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

Information Security Continuity (ISO 27001 Reference: A.17.1)

- The Company must demonstrate that they maintain processes, procedures and controls to ensure the required level of continuity for information security during

an adverse situation and shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Security Requirement Check List

Confidentiality Requirements

City of Toronto(COT) is bound to comply with the Privacy and Security Requirements to protect confidential data including but not limited to Personally Identifiable Information. As such, Company shall work with COT to ensure ongoing confidentiality, integrity, and availability of COT Data in the Company's care, and agrees to:

a. Provide COT Data to COT as requested within a predefined period of time mutually agreed upon between COT and Company.
b. Encrypt confidential records (as required by Privacy and Security Requirements) at rest and in transit.
c. Not to access or allow third parties to access, Personally Identifiable Information unless expressly permitted by COT, or COT determines, in its sole discretion, that access is permitted under the Privacy and Security Requirements.
d. Not to directly or indirectly use, collect, disclose, or destroy any Personally Identifiable Information for any purposes that are not required to provide the services or materials or are not authorized by COT.
e. Cooperate with and assist COT to comply with COT's obligations under the
Privacy and Security Requirements.
f. Meet prescribed requirements for security testing (see Operations Security Section).
g. Return to COT any Personally Identifiable Information and Confidential Information in Company's care upon termination of the Agreement.
h. Provide a certificate of destruction to COT where services or components in Company's care are decommissioned within a predefined period of time agreed upon between COT and Company, and within 30 days of termination or expiration of the Agreement; for greater clarity, the certificate of destruction is a written statement issued and signed by a person authorized to legally bind the Company stating that Personally Identifiable Information/Confidential Information and all COT related data in Company's possession has been destroyed;
i. Ensure sufficient protection of credit card or branded debit card information as part of the Deliverables in accordance with relevant Privacy and Security Requirements. e.g., PCI DSS (Payment Card Industry Data Security Standard).

Information Security Requirements for Procurement, Contracts, Solution Design.

The Company shall ensure its Deliverables, whether destined for installation on COT premises or externally hosted/in the cloud, has security controls implemented at the network, application and endpoint layers, including at a minimum, but not limited to: network and host-based firewalls providing Layer 7 (of the Open Systems Interconnection model) application threat detection and mitigation (e.g. Web Application Firewall, Intrusion Detection & Prevention System, antimalware/antivirus, operating system hardening and locking down, patching and vulnerability management, and access controls). In general, the overall security architecture shall be based on Defense in Depth architectural model, using a layered approach as defined in IEC-62443 1-1

Verification of security controls must be in writing to COT through a SOC 2 (Systems and Organizations Controls) Type II report, ISO 27K certification report, or other document attesting to the industry standard security controls in the hosted provider environment, with respect to all Deliverables components including COT data in the Company's care.

(1) **Protection of the Perimeter:**

a. Communications from lower Security Zones to higher Security Zones shall be done using a properly configured (iDMZ) Industrial DMZ and firewall using best practices as outlined by NIST SP 800-82 and IEC-62443. No external access shall be allowed within the critical networks. Firewall rules will permit only connections between the critical network and iDMZ that are initiated by critical network

b. As outlined in IEC-62443 connectivity between zones is subject to principles of adjacency (no zone hopping) i.e., only Security Zones adjacent to one another may initiate or service communication requests. E.g., desktops in the Trusted Client Zone cannot directly initiate a session with the application data stored in a server in the Restricted High Security Zone as they are not adjacent

c. Where inter-zone communications are required, communications shall be initiated from higher Security Zones to lower Security Zones. Zone separation will be achieved through adequate means such as a properly configured stateful inspection firewall, and appropriately placed and configured intrusion detection devices and use of proxies where appropriate. Traffic should originate from critical networks outbound in uni-directional manner to external networks.

d. Ensure that Intrusion Prevention Systems are implemented on networks with connectivity to the Internet and networks with sensitivity zones and/or trust boundaries.

e. Within a given Security Zone, there are additional segments or partitions. The segmentation of networks within a zone will be accomplished through the use of VLANs. These segments are used to isolate different classes of hosts that have no requirement to interact with each other or instead of VLANs, host-based firewalls may be used to protect hosts within a common Zone (Intra-Zone). This principle of least privilege helps to contain the damage in the event that any given system is compromised.

f. Implement appropriate security controls to ensure the integrity and confidentiality of data flowing across the network and between the zones.

Company must provide a response to this document to the COT,

a. As part of its RFP response during the procurement process; and
b. Annually (at minimum), throughout the term of the Agreement.

Information Security Policies

a. The Company's information security policies, practices and Deliverables design must be in accordance with information security industry standards and frameworks, including but not limited to the latest versions of: ISO 27000 family of standards and the ISO 27002 Code of Practice, the National Institute of Standards and Technology (NIST), ISA IEC 62443, SOC 2 Type II Critical Controls Matrix.
b. The Company and the COT shall work together to ensure that any on premise Deliverable is implemented in accordance with all COT guidelines, work instructions, standards and/or policies including change and configuration policies and standards.

Information Security Organization

a. The Company shall ensure segregation of duties and areas of responsibility in any hosted environment between COT and the Company, as well as internal to the Company, to reduce exposure of COT data to unauthorized users.
b. The Company shall ensure that only Authorized Parties have access to Personally Identifiable Information and Confidential Information.
c. The Company shall provide specialized training for Authorized Parties with

significant security duties, including but not limited to human resources or information technology functions, and any technology administrator function. At a minimum, specialized training shall include, as applicable to the role, information security procedures, acceptable use of information security resources, current threats to information systems, security features of specific systems, and secure access procedures.

d. The Company shall take reasonable steps to prevent unauthorized access to or loss of Personally Identifiable Information and Confidential Information and the services, systems, devices or media containing this information.
e. The Company shall employ risk assessment processes and procedures to regularly assess systems used to provide services or products to COT. Company shall remediate such risks as soon as reasonably possible and commensurate with the level of risk to Personally Identifiable Information and Confidential Information, given threats known at the time of identification. Operate a process to report risks or suspected incidents to the Company security team.
f. If Company performs services COT facilities or using services, systems, devices, or media owned, operated, or managed by COT, Company shall cause all Authorized Parties to comply with all COT policies made available to Company, upon its request, that are applicable to such access. Company shall promptly notify COT in writing when an Authorized Party no longer needs access to the Personally Identifiable Information or Confidential Information in order for Company to provide products or services to COT, including without limitation, when an Authorized Party is terminated or is otherwise no longer performing services under the Agreement.
g. The Company shall require non-disclosure or confidentiality contractual commitments from Authorized Parties before providing them with access to Personally Identifiable Information and Confidential Information.

Human Resource Security

a. The Company shall ensure there are sufficient controls on Company's' personnel with access to COT data in the hiring lifecycle including:
    - Screening/onboarding staff.
    - Terms of employment (during employment and upon termination) to ensure protection of Personally Identifiable Information and Confidential Information.

- A pre-established asset return policy upon termination of personnel and /or expiration of business relationship.

Physical and Environmental Security

a. Physical access to Company and subcontracted third party hosted facilities must be secured from unauthorized users.
b. Physical access to Company and subcontractor facilities must be monitored; access must be logged and auditable in both human readable and machine readable (e.g., System Logs/Syslog) formats, covering the following as minimum:
    - Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms
    - Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.
c. The Company shall ensure physical environmental controls are in place to protect its hosted environment and Deliverable's components housing or processing COT Data. These include but are not limited to Heating Ventilation & Air Conditioning systems (HVAC), fire suppression, equipment rack fans and power system protection.

Access Control

a. The Company shall provide an access control methodology that supports secured remote connections to the system. Remote connections shall be made available exclusively for maintenance & system support.
b. Deliverables must employ strong, industry standard authentication methods and schemes including multi-factor authentication where applicable. Access must be granted only to employees and authorized parties who require such access to perform their job functions / roles (i.e., role-based access).
c. Deliverables must have configurable layers of authorization, authentication, and permissions to ensure adherence to the Principle of Least Privilege to restrict data disclosure. They must also include authorization, authentication, and permissions detailed logging with log retention timelines acceptable to COT.
d. Deliverables including software and hardware must be able to support Single Sign On (SSO) for authentication based on industry standards and best practices, as applicable to the Deliverables.
e. Remote access and virtual private networks (VPNs) established between Company and COT, and connecting any external parties used by Company to host COT data must be implemented with a secure industry standard protocol (*e.g.,* IP Security/IPsec, Secure Sockets Layer/SSL), using the strongest industry standard encryption reasonable and as applicable to implement in the Deliverables. The Company will work the COT to ensure that the VPN setup and configuration is acceptable to the COT.
f. All remote and local users must use strong credentials for authentication with clear text/weak cipher protocols are disabled and not used for any data transfer.

g. Company to ensure with Remote access that split tunnelling is not enabled while connected to the COT network.
h. Two or Multi factor authentication must be used as applicable to the Deliverables.
i. The Company shall document the levels, methods, and capabilities for authentication and authorization. The Company shall deliver a product that adheres to standard authentication protocols. Additionally, the Company provided product shall include audit logging capabilities for all authorization and authentication methods.
j. Unless specifically requested by the COT, the Company shall not allow multiple concurrent logins using the same authentication credentials, allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins.
k. The Company shall prevent critical Operations Technology (OT) components in the OT environment from direct communications to and from the internal COT or external environments by using proxy servers, intermediary services or equivalent ideally in the Industrial Demilitarized Zone (iDMZ). Administrative access to System devices in this infrastructure needs to have their administrative functions limited to minimize risk of unauthorized users accessing these systems. Connections shall be limited to Local and remote access to the devices should be limited to only authorized COT personnel with role-based user privilege levels defined exclusively in line with requirements of job.
l. Access credentials provided by the COT to any individual must not be shared without express permission from the COT. The COT reserves the right to disable the use of any account found to be in use by someone other than the authorized user.
m. Application access provided by a Company intended for authorized COT users must use the most secure industry standard with respect to session protocols and credentials where applicable. The Company must provide details for approval by the COT.
n. Logical access to systems, web portals, software/applications, other points of user manipulation/interaction in the Deliverables must be logged and auditable in both human readable and machine readable (*e.g., System Logs/*Syslog) formats.

Identification and Authentication

a. The Company shall assign unique user IDs to individual users and assign authentication mechanisms to each individual account.
b. The Company shall use a documented user ID lifecycle management process including, but not limited to, procedures for approved account creation, timely account removal, and account modification (e.g., changes to privileges, span of access, functions/roles) for all access to Personally Identifiable Information and Confidential Information and across all environments (e.g., production, test, development, etc.).
c. The Company shall restrict all access to Personally Identifiable Information and

Confidential Information to those using a valid user ID and password and require unique user IDs to employ one of the following: password or passphrase, two-factor authentication, or a biometric value.

d. Each of the solution's "layers" must implement a strong password policy. The policy will be applied for all users and Company staff accounts and will include the following:
    - A minimum password length
    - Complexity enforcement
    - Prohibit the use of previous passwords.
    - A password minimum and maximum age (expiry) for, at least, administrative roles.
e. The Company shall verify user's identity and set one-time use and reset passwords to a unique value for each user. Systematically prompt change after first use.
f. The Company shall use a secure method for the conveyance of authentication credentials (e.g., passwords) and authentication mechanisms (e.g., tokens or smart cards).
g. The Company shall use an authentication method based on the sensitivity of Personally Identifiable Information and Confidential Information. Whenever authentication credentials are stored, must protect all authentication credentials using a strong encryption/hashing algorithm.

Information Systems Acquisition, Development and Maintenance

a. The Company shall follow industry-standard development procedures, including separation of access and code between non-production and production environments and associated segregation of duties between such environments.
b. The Company shall ensure internal information security controls for software development are assessed regularly and reflect industry best practices, and revise and implement these controls in a timely manner.
c. The Company shall manage security of the development process and ensure secure coding practices are implemented and followed, including appropriate cryptographic controls, protections against malicious code, and a peer review process.
d. All software, GUIs and web sites/portals provided for COT use by the Company are expected to have been developed to the most current Open Web Application Security Project (OWASP) secure coding and design.
e. The Company shall disclose features (including administrative backdoors etc.) in software and hardware delivered by the Company for use by the COT.
f. Malware and virus protections must be undertaken (system hardening, patching, scanning) prior to being delivered to the COT.
g. Company shall work with COT to define roles and responsibilities between the

parties in the contract to ensure that ongoing patching, upgrade paths and vulnerability management is defined and assured for the Company provided hardware and software during the contract lifecycle and/or post warranty as negotiated.

Data Governance

a. Data must not be extracted or used outside the solutions' production environment (e.g., QA, Development) without applying proper techniques first to de-personalize the information (e.g., scrubbing, masking).
b. The Company shall separate non-production information and resources from production information and resources.
c. The Company shall build and maintain a PCI zone if Company processes or stores card holder data.
d. For applications that utilize a database that allows modifications to Personally Identifiable Information and Confidential Information, have and maintain a database transaction audit logging features enabled and retain database transaction audit logs for a minimum of one (1) year.

Cryptography and Encryption

a. In cases where COT requires Company to provide a cryptographic system for key management, policies and procedures shall be established for the management of cryptographic keys in the cryptosystem, which covers following as minimum:
    - Cryptographic keys management lifecycle from revocation and replacement
    - Cryptographic protocol and algorithms used
    - Access controls for key generation
b. Encryption keys and salt values for hashing (e.g., protect passwords and other sensitive information) must be stored and managed securely.
c. Upon request from COT, Company shall inform COT of changes within the cryptosystem, especially if the COT's data is used as part of the service, and/or the COT has some shared responsibility over implementation of such controls.
d. All encrypted tunnels in the Deliverables, between the Company, COT and users must use industry standard, latest version of Federal Information Processing Standards (FIPS) 140-x encryption schemes. Use of proprietary encryption protocols must be disclosed and approved by COT.
e. Wireless network and other related components in the Deliverables must adhere to industry wireless standards. Use of proprietary or consumer grade equipment and configuration must be disclosed and approved by COT.
f. The Company shall use a strong encryption/hashing algorithm (with no known vulnerabilities/weaknesses) to protect Personally Identifiable Information and Confidential Information when stored.
g. The Company shall use a strong encryption/hashing algorithm (with no known vulnerabilities/weaknesses) for the transfer of Personally Identifiable Information

and Confidential Information outside of COT-controlled or Company-controlled networks or when transmitting Personally Identifiable Information and Confidential Information over any untrusted network.

Monitoring

- The Company shall retain log data for Personally Identifiable Information and Confidential Information for at least 12 months from the date the log data was created and make the log and such data available to COT within a reasonable timeframe and upon request, unless specified elsewhere in the Agreement. Logs shall be designed to detect and respond to incidents and include, but not be limited to:
    - All individual user access to Personally Identifiable Information and Confidential Information
    - All actions taken by those with administrative or root privileges
    - All user access to audit trails
    - Invalid logical access attempts
    - Use of and changes to identification and authentication mechanisms

- The logs must be monitored and have the capability of alerting the Company and/or the City of Toronto of any suspicious account activity, unauthorized access or suspicious operations (e.g., unauthorized access attempts, violation of usage, general control failures, anomalies in normal operations).
    - Restrict access for security logs to authorized individuals and protect security logs from unauthorized modification.
    - Implement a change detection mechanism (e.g., file integrity monitoring) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; configure software to perform critical file comparisons weekly.
    - Daily review all security events, logs of system components storing, processing, or transmitting card holder data, logs of critical system components, and logs of servers and system components performing security functions.

Communications Security

a. Unless otherwise required by COT, keep COT Data in a physically secure and separate location (logically or physically) safe from loss, alteration, destruction and to implement, use and maintain appropriate policies, standards, products, tools, measures, and procedures to do so in accordance with Privacy and Security Requirements.
b. All Personally Identifiable Information and Confidential Information exchanged between the Company and COT must be encrypted, as applicable. This must use the strongest viable industry standard encrypted session protocol *e.g.,* Transport Layer Security v1.2+.

c. The Company shall work with the COT to facilitate network connectivity to the hosted infrastructure and/or COT resources via secure protocols following industry standards.

Operations Security

a. The Company must perform, upon COT request, vulnerability assessments/security assessments of the hosted infrastructure and provide COT evidence of such tests. The assessments shall comply with all applicable industry standards for security (e.g., Open Web Application Security Project/OWASP, Center for Internet Security/CIS, International Organization for Standardization/ISO 27002, etc.). Regardless of the frequency of COT requests, such assessments must be performed annually at a minimum. The Company may employ a third party to perform such testing at the Company's expense. Findings are to be sent to COT in accordance with COT direction.
b. The testing shall include, but not be limited to:
    - Communication Robustness Testing – This shall include, at a minimum, communication protocol fuzz testing to determine the ability to properly handle malformed and invalid messages for all identified communication protocols in the Deliverables, as well as data resource exhaustion tests (aka “load testing” and “DoS testing”). Communication robustness testing shall be performed using tools that are approved by COT, and that produce machine-readable data.
    - Software Composition Analysis – This shall include, at a minimum, an analysis of all compiled code found in the Company product and shall identify all third-party open-source components, and shall, at a minimum, identify all known vulnerabilities found in the Common Vulnerabilities and Exposures (CVE) in publicly available databases. Software composition analysis shall be performed using tools that are approved by COT, and that produce machine-readable data.
    - Dynamic Runtime Analysis – This shall include, at a minimum, an analysis of how the Company provided software behaves during operations and whether such behaviour introduces potential security vulnerabilities that could negatively impact confidentiality, integrity, and availability.
    - Known Malware Analysis – This shall include, at a minimum, a scan of Company provided software to determine if any known malware exists in the Company provided software and a risk assessment on mitigation controls or value of risk.
    - Bill of Materials – The Company shall provide COT a bill of materials that clearly identifies all known third-party software components contained in the Deliverables. This shall be provided in a machine-readable format.
    - Validation of Security Measures – All security measures described in the product’s design documentation are properly implemented and mitigate the risks associated with use of the component or device.
c. Policies and procedures shall be established for labeling, handling, and the security of data and objects, which contain data.

d. Following security testing, the Company is obligated to create a remediation plan acceptable to COT and must implement the remediation plan forthwith at no cost to COT. The Company shall work with COT to minimize impact to COT business and clients e.g. where maintenance windows and Deliverables shall be affected.
e. The Company shall disclose where COT Data will reside, be processed, or be accessed by COT and the Company, and this shall include all confidential data subject to any NDA between COT and Company. The Company will provide advance notification if those jurisdictions change during the life of the contract. Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premise as required.
f. The Company shall work with COT initially, and through the contract lifecycle, when required by law or in response to business changes, to update web portals, application splash screens, privacy policies, and End User License Agreements (EULA) applicable to the Deliverables to properly inform COT users of collection, use, storage, and disclosure of COT Data.
g. Unless otherwise agreed upon between COT and the Company, no Personally Identifiable Information or Confidential Information shall be provided to the Company for use in a development or test environment
h. The Company shall ensure components and data in the Deliverables are backed up regularly.
i. The Company shall ensure adequate monitoring of the Deliverables to alert COT should an issue arise (see Incident Response & Management below).

Incident Response & Management

a. In case of a security or privacy breach the Company shall immediately notify the COT. The Company must also keep the COT informed as they verify the breach and the impact.
b. The Company shall, working within existing breach response plans, provide support during a security breach to help the COT identify, contain, remove, and recover threats during a security incident. COT will retain the right to aid in the investigation of these incidents.
c. As part of Incident response and management, Company shall produce a framework covering the following based on industry standards of each item:
    - Chain of custody document (based on admissible chain of custody management processes and control).
    - Techniques of legally collecting forensic data and analysis procedures.
    - Statistical information for security incident data with COT upon request.

Business Continuity Planning

a. Company shall work with COT within the contract lifecycle to plan, document, execute and test business continuity planning and disaster recovery plans on an ongoing basis and shall produce a defined documented method of determining the impact of any possible disruption and shall work with COT to incorporate the following (but not limited to):

- Identify critical products and services
- Identify all dependencies, including processes, applications, business partners, and third-party service providers
- Establish and document the maximum tolerable period for disruption
- Establish and document the priorities for recovery
- Establish and document recovery time objectives (RTO) and recovery point objective (RPO) for resumption of critical products and services within their maximum tolerable period (MTP) of disruption

b. Additionally, Company shall document all policies and procedures related to retention period of any critical assets which is part of the solution per established policies and procedures as well as applicable legal, statutory, or regulatory compliance obligations.
c. Company shall produce a Backup and recovery measures deliverable as part of the complete package and shall be incorporated appropriately as part of business continuity planning which mirrors the evidence with tests accordingly for effectiveness.

Obsolescence Management

a. The Company shall provide COT with all market-ready equipment hardware and software upgrades, patches, configuration files, and firmware updates at no additional cost.
b. Any patches/upgrades to a Company system(s) would be first tested in the Company's facility prior to the implementation to ensure the expected functionality is achieved.
c. Upon request by the COT, these upgrades shall be installed by the Company via a remote secure connection provided by COT. In the event the installation cannot be performed via remote connection, the Company shall supply the encrypted software on a non- returnable portable device.
d. The Company shall provide an Obsolescence Management Program ("Program"), updated annually, and designed to minimize the effect of any obsolete components. The Program shall include an Annual Equipment Audit providing notice of any component approaching obsolescence within two years of the audit.
e. For any component approaching obsolescence, the Company shall provide:
    - The nearest match available from a new OEM product family.
    - A direct match from the Company's repaired inventory.
    - The closest match from the superseded component's product familiar fit/form/function replacement shall include a write-up of the replacement component, including any modified functionality

Vulnerability and Risk Assessment

a. The Company shall submit as part of the submittal defined in the contract a Threat, Vulnerability and Risk Assessment (TVRA)/Threat model report covering

all critical and non-critical systems/sub-systems for:
    - Associated risks
    - Countermeasures applied
    - Risk mitigation results for all system levels
b. The report shall cover the following as appropriate but are not limited to:
    - Physical access restrictions to OT including all control systems.
    - Physical access restrictions to data in transit and at rest for all on-board and wayside systems.
    - Restrictions applied to wired and/or wireless systems communication to and from wayside to on-board.
    - Centralized system management details for the management of encryption and crypto systems.
    - IT/OT isolation plan for all the critical systems.
    - All application details related to secure coding practices.

Asset Management

a. All Company staff with access to COT assets may be required to sign a Non-Disclosure Agreement (NDA) or other formal written acknowledgment and acceptance of COT policies prior to being given access to COT.
b. Use of Company assets on any COT network is subject to review by COT prior to connection. The Company shall work with COT to harden, lock down, and otherwise secure their assets to COT's satisfaction and, where this is not feasible for either party; the Company may be provided a COT asset for its use.
c. The electronic transfer of Personally Identifiable Information and confidential information between the Company and COT shall be performed through secure COT approved mechanisms with appropriate access security controls. Additionally, physical media must be encrypted while in transit.
d. The Company must be assessed to assure they meet or exceed all COT information security policies, standards, legal and regulatory requirements as part of the contract negotiation process. For new services proposed with currently Company, a security assessment should be performed where the new service differs in scope from other existing services.
e. The Company must maintain and keep updated on a centralized asset inventory at least an annual basis.

Compliance and Accreditations

a. The Company shall be responsible for activities and costs associated with maintaining ongoing Payment Card Industry Data Security Standard (PCI DSS) compliance for components in the Company's environment, products/services as applicable to the Deliverables.
b. All hardware, software, and firmware included as part of the finished product(s) shall comply with cyber security practices current at the time of delivery and consistent with cyber security frameworks such as those defined by the International Standardization Organization (ISO), the National Institute of Standards and Technology (NIST), International Information Systems Security

Certification (ISC2), or Information Technology Infrastructure Library (ITIL).

c. The Company represents and warrants that it performs security testing and validation for all of its products, and that all security testing performed by the Company covers all issues noted in the “SANS/CWE Top 25” and “OWASP Top 10” publicly available lists.
d. Upon COT’s request, certify it is in compliance with this document along with supporting certifications for the most recent versions of PCI-DSS, ISO 27001/27002, SOC 2, or similar assessment for the Company and for any subcontractor or third-party processing, accessing, storing, or managing on behalf of the Company. If the Company is not able to certify compliance, it shall provide a written report detailing where it is out of compliance and its remediation plan to become compliant.