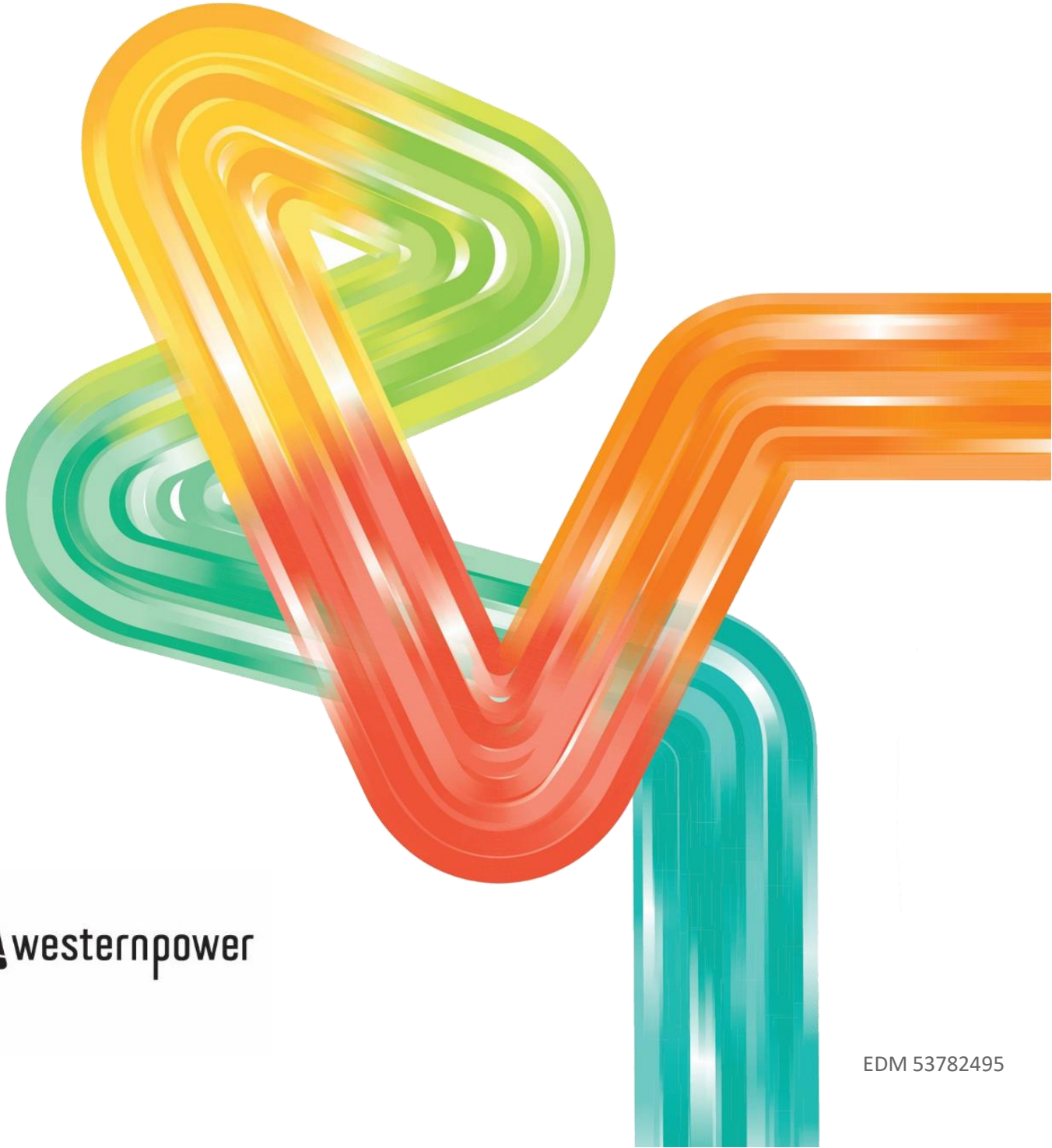
Cyber Security

Vendor's Requirements Guide

4 September 2020



westernpower

EDM 53782495

An appropriate citation for this paper is:

Cyber Security

Western Power

363 Wellington Street
Perth WA 6000
GPO Box L921 Perth WA 6842

T: 13 10 87 | Fax: 08 9225 2660
TTY 1800 13 13 51 | TIS 13 14 50

Electricity Networks Corporation
ABN 18 540 492 861

enquiry@westernpower.com.au
westernpower.com.au

Table of Contents

1. Brief description

The objective of this document is to provide all the necessary information for vendors who provide products and services for Western Power's data networks to meet Western Power's Cyber Security requirements.

1.1 Related Documents

This document supports the vendor in complying with Western Power's Cyber Security Standard (EDM#33923497) and operates alongside Supplier Performance & Relationship Management Standard (EDM #46730860).

1.2 Scope of Document

This document applies to:

i. All contractors and vendors of Western Power when providing goods or services on behalf of Western Power.

ii. All Western Power's business activities and operations.

2. Instructions to Vendors

Vendors are expected to help protect the confidentiality, integrity, and availability of Electricity Networks Corporation (Western Power) data and systems, regardless of how the data is created, distributed or stored. Vendors' security controls can be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal obligations.

Please note that if a vendor processes, stores or transmits Western Power data that is considered "confidential or highly confidential," additional data protection controls may be required.

3. Requirements

Western Power will clarify what requirements below are applicable to vendors. Vendors are expected to refer to information in this section when requested to complete the Cyber Security Checklist for Vendors.

3.1 Cyber Security Program Management (PM)

Vendor implements Cyber Security program management controls to provide a foundation for the Vendor's Information Security Management System (ISMS).

3.1.1 CYBER SECURITY PROGRAM

a) Cyber Security Policy:

Vendor has a documented Cyber Security Standard in place which meets applicable industry standards. This standard can be reviewed on a regular basis by vendor.

b) Cyber Security Management:

Vendor's cyber security program documents the policies, standards, and controls in use that relate to the requirements defined in this document. This security plan includes organizational, administrative, technical, and physical safeguards and standards appropriate to the size and complexity, the scope of the activities and the sensitivity of the information at issue.

c) Management Commitment:

Vendor has the executive-level direction on Cyber Security and be able to demonstrate management commitment.

3.1.2 CYBER SECURITY GOVERNANCE

a) Contract:

Vendor clarifies contract, statement of work, or purchase order queries with Western Power before they manage, collect, use, transfer or store Western Power business information or systems.

b) Cyber Security Function:

Vendor has an established Cyber Security function that has Vendor's enterprise-wide responsibility for promoting Cyber Security.

c) Western Power-Specific Security Coordination:

Vendor appoints an individual to coordinate the Cyber Security arrangements specific to Western Power.

d) Cyber Security Audit / Review:

The Vendor performs independent and regular security audits/reviews on its Cyber Security program.

e) *Cyber Security Architecture:*

Vendor has a Cyber Security architecture that provides a framework for the application of standard security controls for aspects of the vendor's enterprise that deliver products and/or services to Western Power.

Vendor documents relevant data flows (e.g., ports, protocols and services) through network diagrams and/or Data Flow Diagrams (DFDs).

3.1.3 COMPLIANCE

a) *Statutory / Regulatory / Contractual Compliance:*

Vendor maintains a process to be aware of and be compliant with all applicable statutory, regulatory and contractual compliance requirements.

b) *Compliance Status:*

Vendor has a process to document non-compliance of any statutory, regulatory or contractual requirement.

- Vendor identifies and quantifies the risks and mitigation plans and documents the business decision for alternate controls or risk acceptance; and
- The mitigation plan and business decision can be signed off by an authorised individual who can accept responsibility and accountability on behalf of the vendor.

c) *Breach Notification:*

Vendor maintains a documented breach notification process that meets all applicable legal and contractual requirements as mentioned in the contract.

3.1.4 HUMAN RESOURCES SECURITY

a) *Requirements for Employment:*

Vendor must maintain contractual agreements with employees, contractors, consultants and/or other third-party staff that formally documents their responsibilities for Cyber Security as mentioned in the contract.

b) *Roles and Responsibilities:*

Vendor defines and documents security roles and responsibilities of employees, contractors and third-party users to incorporate Western Power's cyber asset protection control requirements:

- Vendor notifies its employees, contractors, and third-party users of the consequences for not following its security policy in handling Western Power data.
- Vendor protects all assets used to manage or store Western Power data, against unauthorised access, disclosure, modification, destruction or interference.

- Vendor provides education and training on security procedures and the correct information processing requirements to its employees, contractors and third-party users.
- Vendor provides additional data protection and privacy training to its personnel with access to sensitive Personally Identifiable Information (PII). Refresher training can be scheduled at least on an annual basis.

c) Assigned Ownership:

Vendor assigns ownership of critical and sensitive information, business applications, computer systems and networks to individuals (e.g., business managers) and documents the responsibilities of these assigned owners.

d) Personnel Screening:

Vendor ensures a secure workforce by doing background verification checks on its candidates for employment and can be carried out in accordance with business requirements, relevant laws, regulations, and ethics.

e) Staff Agreements:

Vendor establishes agreements with its employees that specify Cyber Security responsibilities.

3.2 Access Control (AC)

Vendor implements logical access controls to limit access to systems and processes to authorised users.

3.2.1 LOGICAL ACCESS CONTROL

a) Access Control:

Vendor restricts access to the application and associated information to authorised individuals. This is enforced accordingly to ensure that only authorised individuals to gain access to business applications, systems, networks and computing devices, that individual accountability is assured and to provide authorised users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

b) User Authorisation:

Vendor ensures that all users have authorisation before they are granted access privileges.

- User access privileges are reviewed at least every six (6) months; and
- Access is revoked within twenty-four (24) hours of a user's change in role or employment status.

c) User Authentication:

Vendor ensures strong user authentication is implemented throughout the Vendor's enterprise:

- All users are authenticated by an individual identifier, not group or shared identifiers; and
- Strong authentication mechanisms are used in conjunction with the identifier (e.g., strong passwords, smart cards or biometric devices) before the user can gain access to systems or data.

3.2.2 PRIVILEGED ACCOUNT MANAGEMENT

a) Privileged Accounts:

Vendor ensures that accounts with privileged access are separate from a user's normal, non-privileged account.

3.2.3 OFF-SITE LOGICAL SECURITY CONSIDERATIONS

a) Off-Premise Access Control:

Whenever technically feasible, vendor ensures cloud solutions offer the option to be federated to Western Power systems for authentication using Western Power credentials.

3.3 Awareness and Training (AT)

Vendor ensures that users are made aware of the security risks associated with their roles and that users understand the applicable laws, policies, standards, and procedures related to the security of systems and data.

3.3.1 SECURITY AWARENESS PROGRAM

a) Cyber Security Awareness:

Vendor's employees, contractors, consultants and/or other third-party staff are made aware of the key elements of Cyber Security, why it is needed, and understand their personal Cyber Security responsibilities. A security awareness program is undertaken to promote security awareness to all individuals who have access to the information and systems of the vendor's enterprise.

The security awareness program includes key threats in the vendor's industry that may apply to Western Power

Vendor's security awareness training program provides verifiable data by way of documentation — including training session attendance lists, certificates of completion, documented proof of teachable moments.

3.3.2 SECURITY TRAINING

a) Cyber Security Education:

Vendor's employees, contractors, consultants and/or other third-party staff are trained to run systems correctly, as well as to develop and apply security controls through trainings and cyber security certifications.

E.g, Relevant industry certifications

3.4 Audit and Accountability (AU)

Vendor creates, protects, and retains system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorised, or inappropriate activity by ensuring that the actions of individual users and systems can be uniquely traced.

3.4.1 EVENT LOGGING

a) Event Logging:

Vendor logs all key Cyber Security events, including but not limited to:

- All actions taken by any individual with root or administrative privileges;
- Access to all audit trails;
- Invalid logical access attempts;
- All individual user accesses confidential or highly confidential data;
- Use of and changes to identification and authentication mechanisms, including but not limited to:
- Creation of new privileged accounts and elevation of privileges; and
- All changes, additions, or deletions to accounts with root or administrative privileges;
- Initialisation, stopping, or pausing of the audit logs; and
- Creation and deletion of system-level objects.

b) Intrusion Detection / Prevention:

Vendor implements and monitors Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) mechanisms on all critical systems and networks.

3.4.2 MONITORING & REVIEW

a) System Network Monitoring:

Vendor develops and implements a process to review logs and security events for all system components to identify anomalies or suspicious activity that includes:

Reviewing the following, at least daily:

- All security events;
- Logs of all system components that store, process, or transmit cardholder data, or that could impact the security of cardholder data;
- Logs of all critical system components; and
- Logs of all servers and system components that perform security functions. This includes, but is not limited to:
  - Firewalls;
  - Intrusion Detection Systems (IDS);

- Intrusion Prevention Systems (IPS); and
- Authentication servers (e.g., Active Directory domain controllers); and
- Following up exceptions and anomalies identified during the review process.

3.5 Security Assessment and Authorisation (CA)

Vendor periodically assesses systems to determine if IT security controls are effective and ensure IT security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

3.5.1 CONTROL TESTING

a) Testing:

Vendor ensures that all elements of a system (e.g., application software packages, system software, hardware, and services) are rigorously tested before the system is promoted to a production environment.

b) Test Data:

Vendor ensures any sensitive Western Power business information copied from the production environment is protected by:

- Depersonalising sensitive business information;
- Restricting access to business information in the development environment; and
- Erasing copies of Western Power business information once testing is complete.

c) Post-implementation Review:

Vendor ensures a post-implementation review is conducted for all deployed or commissioned systems to the production environment.

3.6 Configuration Management (CM)

Vendor maintains accurate inventories of its systems and enforce security configuration settings for information technology products employed in support of its business operations.

3.6.1 CONFIGURATION MANAGEMENT

a) *Configuration Management:*

Vendor implements configuration standards for all system components that address known security vulnerabilities and are consistent with industry-accepted system hardening standards.

3.6.2 CHANGE MANAGEMENT

a) *Change Control:*

Vendor documents and manages operating procedures for its change control process(es).

b) *Change Management:*

Vendor ensures that changes to any systems, applications or networks, including “emergency” changes, are reviewed, tested, approved and applied using a change management process.

c) *Change Documentation Retention:*

Vendor ensures that documentation of changes is retained for at least 7 years.

3.7 Contingency Planning (CP)

Vendor establishes, implements and maintains plans for the continuity of operations (COOP) in emergency situations to ensure the availability of critical information resources.

3.7.1 BUSINESS CONTINUITY & DISASTER RECOVERY

a) Business Continuity & Disaster Recovery:

Vendor develops, supports and routinely tests a viable Business Continuity and Disaster Recovery (BC/DR) plan that addresses all reasonably-foreseen contingency arrangements.

b) Resilience:

Vendor's applications, systems, and networks are run on robust, reliable hardware and software, supported by alternative hardware or duplicate facilities.

c) Data Backups:

Vendor ensures that backups of essential information and software are performed on a regular basis, according to a defined cycle discussed with and approved by Western Power.

3.8 Identification and Authentication (IA)

Vendor implements mechanisms to properly identify system users, processes acting on behalf of users or devices, and authenticate the identities of those users, processes, or devices.

3.8.1 USER ACCOUNTS

a) User Identification:

Vendor assigns all users a unique identification (ID) before allowing them to access systems. In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Something you know, such as a password or passphrase;
- Something you have, such as a token device or smart card; or
- Something you are, such as a biometric.

b) Unique Accounts:

Vendor ensures proper user identification and authentication management for all standard and privileged users on all systems, as follows:

- Ensure that only authorised users are provided with user IDs;
- Ensure that usernames and service accounts are uniquely named and, in a manner, consistent with organisationally defined Guide s; and
- Require written authorisation by a supervisor or manager to receive a user ID.

c) Privileged Users:

Where technically feasible, Vendor implements multifactor authentication for the system and network access from privileged accounts.

3.8.2 PASSWORD MANAGEMENT

a) Password Management:

Vendor enforces strong passwords for all user and service accounts.

- Password are not present in any public database of known breached credentials
- Setting Passwords is aligned with Western Power's Password setting policy

3.9 Incident Response (IR)

Vendor establishes an actionable IT security incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

3.9.1 CYBER SECURITY INCIDENT MANAGEMENT

a) Incident Management:

Vendor documents all Cyber Security incidents and maintains a documented Cyber Security event management process that covers the incident response, escalation, and remediation of Cyber Security events and incidents.

b) Reporting Incidents:

Vendor informs Western Power without delay about any Cyber Security incident that could have an impact on Western Power's business operations with the vendor.

c) Integrity Requirements:

Vendor assesses and immediately escalates to Western Power about the impact of business information being accidentally corrupted or deliberately manipulated. The analysis of integrity requirements determines how the accidental corruption or deliberate manipulation of information could have an impact on Western Power's business operations with the Vendor.

d) Availability Requirements:

Vendor assesses and immediately escalates to Western Power about the impact of business information being unavailable for any length of time. The analysis of availability requirements i determines how a loss of availability of information could have an impact on Western Power's business operations with the vendor.

e) Forensic Investigations:

Vendor has an established process for managing incidents that require forensic investigation, since it is the vendor's responsibility to preserve evidence and maintain the chain of custody for incidents within the vendor's areas of responsibility.

3.10 Maintenance (MA)

Vendor performs periodic and timely maintenance on systems, so that Western Power assets are protected from the latest threats.

3.10.1 MAINTENANCE

a) Maintenance:

Vendor schedules, performs, documents, and reviews records of maintenance and repairs on systems in accordance with manufacturer or vendor specifications and company requirements; such as:

- Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- Require explicit management approval for the removal of the systems or system components from company facilities for off-site maintenance or repairs;
- Sanitise equipment to remove all information from associated media prior to removal from company facilities for off-site maintenance or repairs; and
- Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

3.10.2 VULNERABILITY MANAGEMENT

a) Vulnerability Management:

Vendor ensures a vulnerability management program exists to eliminate vulnerabilities that could be exploited by malware or other technical methods (e.g., exploitation through technical vulnerabilities). This includes, but is not limited to:

- Vulnerability remediation;
- Software and firmware patching; and
- Hardware maintenance.

b) Web-Enabled Applications:

Vendor implements and manages specialised technical controls for web-enabled applications to ensure that the increased risks associated with web-enabled applications are minimised:

- All internet facing websites are scanned for security vulnerabilities that potentially open the site up to malicious behaviour.
- Western Power's minimum list of validation is the Open Web Application Security Project (OWASP) Top 10 vulnerabilities (e.g., cross-site scripting (XSS), SQL injection, Admin access, open directories, insecure data transfer, etc.).

3.11 Media Protection (MP)

Vendor protects system media, both hardcopy and digital, by limiting access to authorised users and sanitising or destroying media so that unauthorised data recovery is technically infeasible.

3.11.1 DATA CLASSIFICATION

a) Classification:

Vendor utilises a Cyber Security classification scheme that applies throughout the vendor's enterprise.

3.11.2 ASSET & MEDIA HANDLING

a) Asset Management:

Vendor manages essential information about hardware, software, and data flows/extracts/interfaces (e.g., unique identifiers, version numbers, data recipients, physical locations) in inventory:

- Western Power will generally inform the Vendor of the classification of Western Power data provided to Vendor. In the event Vendor is not certain of the classification of any item of Western Power data, Vendor will seek clarification from its Western Power business contact.
- An appropriate set of procedures for labelling and handling is developed and implemented by Vendor.
- Personal use of Western Power equipment and data is not allowed.

b) Handling Information:

Vendor ensures additional protection is provided for handling sensitive material or transferring sensitive information.

- Files containing personal information or business sensitive information are transferred (e.g., email, faxes, etc.) via secure/encrypted file transfer protocols;
- Sensitive information is encrypted on all devices, including portable devices, such as laptops, portable media (flash drives) and data backups; and
- Western Power's minimum encryption requirement is 128-bit AES.

3.11.3 RETENTION & SECURE DESTRUCTION

a) Records Retention:

Vendor maintains a formal records retention program.

b) Secure Destruction:

Vendor ensures methods of destruction are formally implemented, based on the type of media:

- Physical, paper-based media;
- Physical, digital media; and
- Electronic, digital data

3.12 Physical & Environmental Protection (PE)

Vendor implements physical access controls to limit access to systems, equipment, and the respective operating environments to authorized individuals. Vendor will provide appropriate environmental controls in facilities containing Western Power systems.

3.12.1 PHYSICAL PROTECTION MEASURES

a) Facilities:

Vendor secures facilities where Western Power data is stored, processed or transmitted:

- The number of entrances to the information processing facilities in which Western Power data is stored is limited.
  - Every entrance into these areas requires screening. (e.g., security guard, badge reader, electronic lock, a monitored closed caption television (CCTV)).
  - Access logs is recorded and maintained.
- Physical access is restricted to those with a business need.
  - Access lists is reviewed and updated at least once per quarter.
- Process, training, and policies are in place to determine visitor access, after-hours access, and prevent tailgating into controlled areas.
- Emergency exits in controlled areas to sound an alarm when opened and include automatic closure.
  - Any alarms to trigger an emergency response.

b) Physical Protection:

Vendor actively manages the physical security controls and ensures all buildings throughout the Vendor's enterprise that house critical IT functions (e.g., data centres, network facilities, and key user areas) are physically protected from unauthorised access.

c) Hazard Protection:

Vendor ensures computer equipment and facilities are protected against natural and man-made hazards.

d) Power Supplies:

Vendor protects critical computer equipment and facilities against power outages.

3.12.2 PROCESSING FACILITIES

a) Comingling of Data:

Vendor ensures that when Western Power business information is co-located with non-Western Power data, (e.g., virtual servers, cloud solutions, etc.) the non-Western Power data is at least be logically separated from Western Power business information.

b) Physical Location of Data:

Vendor is responsible for notifying Western Power before relocating any physical storage location of Western Power business information to a country different from the one(s) documented in vendor's statement of work or contract so that potential implications for privacy can be addressed.

c) Virtualization & Cloud Solutions:

If Vendor utilises a cloud solution, Vendor adheres to the same security principles required by vendor's IT security policies and applicable government regulations, laws, or directives as used throughout vendor's enterprise:

- The geographic location of provider infrastructure resources is made clear to Western Power. Western Power can control data location in cloud services to ensure compliance with local laws that restrict the cross-border flow of data.
- Vendors providing cloud services to:
  - Provide a process for data destruction and secure deletion of any and all Western Power data as needed;
  - Have an established method of encrypting sensitive data in storage and in transit following industry-recognized leading practices;
  - Securely handle Western Power related data, compute resources, virtual machines resources by providing logical isolation and secure migration;
  - Include methods or options for multi-factor authentication for cloud administrator roles;
  - Provide Western Power the capability to fully audit Western Power user access and activity within the cloud service. Audit logs must be capable of being exported from the cloud service;
  - Limit employee access to the least privilege needed to perform their duties.
  - Maintain documented audits or established compliance roadmaps in alignment with Industry Standard Certifications for Cloud Security. Examples include ISO27001/2, SSAE16, FEDRAMP, CSA STAR, FIPS 140-2, and Open Data Alliance;

  - Demonstrate adherence to Security Development best practices for all code, APIs, and applications deployed and implemented in support of the cloud service;
  - Process and advise Western Power of any security breach involving Western Power data or services utilized by Western Power; and
  - Provide Western Power with the means to monitor in near real-time service and resource availability; and
- All access to cloud computing sites to encrypt data in transit.
  - Any Western Power data stored in a cloud environment is encrypted either by the Vendor or the application so that data cannot be read by other users in a multi-tenant environment.

3.13 Planning (PL)

Vendor develops, documents, implements, and periodically updates measures to protect its critical systems.

3.13.1 COORDINATION

a) Coordinated Cyber Security Operations:

Vendor plans and coordinates security-related activities affecting the information system potentially affected parties before conducting such activities in order to reduce the impact on other business operations.

3.13.2 RULES OF BEHAVIOR

a) Acceptable Use:

Vendor develops usage policies and defines proper use of Vendor's technologies.

3.14 Personnel Security (PS)

Vendor ensures that published rules of behaviour are followed by users and employs a method of formal sanctions for personnel who fail to comply with IT security policies and standards.

3.14.1 HUMAN RESOURCES SECURITY

a) Cyber Security Roles:

Vendor ensures that all security-related positions are staffed by qualified individuals and those individuals have the skill set necessary to perform the Cyber Security-related job functions.

b) Personnel Screening:

Vendor screens potential personnel prior to hiring to minimise the risk of compromise from internal sources.

c) Personnel Termination:

Vendor ensures that upon termination of a vendor employee' employment system access accounts are disabled with twenty-four (24) hours of the termination action.

d) Confidentiality Requirements:

Non-disclosure agreements are signed by Vendors prior to being granted access to Western Power information.

- Vendor assesses and immediately escalates to Western Power about the impact of business information being accidentally or deliberately released to unauthorised parties.
- The analysis of integrity requirements determines how the disclosure of information could have an impact on Western Power's business operations with the vendor.

3.15 Risk Assessment (RA)

Vendor periodically assesses the risk to operations, assets, and data, resulting from the operation of systems and the associated processing, storage, or transmission of data.

3.15.1 RISK MANAGEMENT

a) Risk Assessments:

Vendor performs information risk assessments of critical areas of its business to identify key information risks and determines the controls required to keep those risks within acceptable limits.

- Assessment includes, but are not limited to:
  - Business environments;
  - Business processes;
  - Business applications (including those under development);
  - Computer systems, and
  - Networks.
- Vendor provides Western Power with a documented analysis of how key threats, as identified above in section 1(a), are addressed, as it applies to Western Power.

3.16 System, Services Acquisition and Development

Vendor allocates enough resources to adequately protect organisational systems by employing a Secure System/ Solution Development Life Cycle (SSDLC) process that incorporate IT security considerations.

3.16.1 SYSTEM ACQUISITION & DEVELOPMENT

a) Supply Chain:

Vendor ensures that reliable and approved hardware and software are acquired that follows consideration of security requirements. Vigilance maintains to prevent counterfeit hardware and software from being used anywhere in the Vendor's enterprise.

b) Specification of Requirements:

Vendor takes into consideration the Cyber Security requirements for the system under development when designing the system to ensure Western Power's business requirements (including those for Cyber Security) are documented and agreed upon before detailed design commences.

c) Quality Assurance:

Vendor ensures quality assurance activities are performed for critical security controls during the development lifecycle.

d) Development Methodologies and Environment:

Vendor's development activities are

- Carried out in accordance with a documented system development methodology;
- Performed in specialized development environments;
- Isolated from production environments; and
- Protected against disruption and disclosure of information.
- Using source code repositories registered and approved by Western Power

e) System Design / Build:

Vendor ensures system build activities are:

- Carried out in accordance with industry-recognized leading practices (e.g., OWASP);
- Performed by individuals provided with adequate skills/tools; and
- Inspected to identify unauthorized modifications or changes which may compromise security controls.

f) Installation Process:

Vendor ensures that systems to be transitioned to the production environment are deployed/commissioned in accordance with the Vendor's documented deployment or commissioning process.

g) Lifecycle Management:

Vendor defines the End of Life (EOL)/End of Support processes for all systems and applications which could include date of EOL/EOS and any business triggers that may result in updated EOL/EOS date;

3.16.2 Vendor MANAGEMENT

a) Outsourcing:

Vendor operates a formal process to address due care and due diligence considerations in the selection and management of third-party Vendors:

- These third-party vendors to sign agreements that specify the security requirements to be met before commencing work on behalf of vendor that could have an impact on Western Power's business operations with the vendor;
- These security requirements are aligned with the provisions expected of Western Power from vendor; and
- All subcontracted activities involving Western Power information are approved and secured by vendor.

b) Vendor Exit Strategy:

Vendor ensures a documented termination of service process is in place that ensures Western Power business data is recoverable if vendor terminates a service agreement with a third-party vendor.

c) Indemnification:

Vendor addresses indemnification considerations with third-party vendors that could have an impact on Western Power's business operations with the vendor.

3.17 System & Communications Protection (SC)

Vendor employs industry-recognised leading practice principles that promote effective IT security within systems and the network.

3.17.1 COMMUNICATIONS & OPERATIONS MANAGEMENT

a) Communications Security:

Vendor supports standards and procedures that ensure confidentiality, integrity, and availability of information and services with continuous oversight on new threats and vulnerabilities by a documented risk assessment process driving risk mitigation implementation on a timely basis.

b) Operations Management:

Vendor maintains enough overall operational control and visibility into all security aspects of how data is processed, stored and transmitted:

- System administrators have adequate training and experience to securely administer the infrastructure within their responsibility;
- Vendor have a separation of duties process to prevent one individual from controlling all key aspects of a critical transaction or business process; and
- Vendors are responsible for data protection, privacy compliance, and security control validation/ certification of their sub-contractors.

3.17.2 CRYPTOGRAPHY

a) Cryptography:

Vendor's cryptographic solutions:

- Meet or exceed Western Power's minimum encryption requirement of 128-bit AES (Subject to Western Power's minimum encryption requirement); and
- Protect the confidentiality of sensitive information that is subject to legal and regulatory-related encryption requirements.

b) Cryptographic Key Management:

Vendor manages cryptographic keys, in accordance with industry-recognised leading practices for key management:

- Documented standards and procedures exist; and
- Cryptographic keys are protected against unauthorised access or destruction to ensure that these keys are not compromised (e.g., through loss, corruption or disclosure).

3.17.3 NETWORK SECURITY

a) Defence In Depth (DiD):

Vendor secures its computer networks using multiple layers of access controls to protect against unauthorised access. In particular, vendor shall:

- Group network servers, applications, data, and users into security domains;
- Establish appropriate access requirements within and between each security domain; and
- Implement appropriate technological controls to meet those access requirements consistently, including (for example) firewalls.

b) Network Controls:

Vendor ensures that all data and communications networks are secured to ensure the transmission of data is kept confidential.

- Applications, ports, services, and similar access points installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed;
- Network segments connected to the Internet are protected by a firewall which is configured to secure all devices behind it;
- Network segments where Western Power data resides are isolated from non-Western Power data, logically or physically unless approved by Western Power Security;
- User connection capability are documented about messaging, electronic mail, file transfer, interactive access, and application access;
- All production servers are in a secure, access-controlled location;
- Firewalls are configured properly to address all reasonably-known security concerns;
- Infrastructure diagrams, documentation, and configurations are up to date, controlled and available to assist in issue resolution; and
- Systems are the ability to detect a potential hostile attack. (e.g., IDS/IPS)
- All systems are updated to the current release and actively monitored.

c) Wireless Access:

Wireless access is authorised, authenticated, encrypted and permitted only from approved locations.

d) Remote Access:

Remote access to a network containing Western Power data is done via a secure connection (e.g., VPN).

- All extranet connectivity into Western Power is through Western Power-approved and authorised secure remote connections.

3.18 System & Information Integrity (SI)

Vendor corrects flaws in its systems in a timely manner and ensures mechanisms are in place to protect systems from malicious code.

3.18.1 MALWARE PROTECTION

a) Malware Controls:

Vendor implements and manages enterprise-wide detection, prevention and recovery controls to protect against malware that includes having procedures and assigned responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks.

b) Malware Prevention:

Vendor ensures the installation and regular update of malware detection and repair software to scan systems and media as a precautionary control, or on a routine basis. The scan carried out includes:

- Scan any files received over networks or via any form of storage medium, for malware before use;
- Scan electronic mail attachments and downloads for malware before use; and
- Scan web pages for malware.

3.18.2 SYSTEM CONFIGURATION

a) Host System Configuration:

Vendors configures host systems according to an industry standard.

- Systems are configured to function as required and to prevent unauthorised actions.
- Examples of best practice configuration include, but are not limited to:
  - Centre for Internet Security (CIS)
  - US Department of Defence Secure Technical Implementation Guides (STIGs)
  - OEM best practices (e.g., Microsoft, VMware, Oracle, etc.)

b) Mobile Devices:

Vendor maintains policies, standards, and procedures covering the use of mobile/portable devices.

- The use of mobile devices (e.g., smartphone, iPad, tablet, USB memory sticks, external hard disk drives, MP3 players, e-book readers, etc.) is:
  - Subject to approval; and

  - Access is restricted.
- Controls are implemented to ensure that sensitive information stored on these devices is protected from unauthorised disclosure.