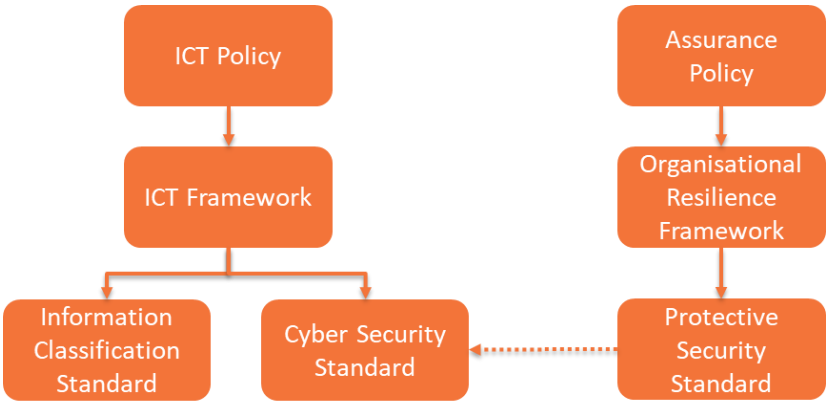
Information and Communication Technology Cyber Security Standard

1. Brief description

This Standard specifies cyber security principles that protects Western Power systems and data from unintended or unauthorised access, damage or destruction.

1.1 Related policies

This Standard is made under and supports the Information and Communication Technology Policy (EDM# 54209633) and complements the Protective Security Standard (EDM# 41485777).



1.2 Introduction

The security and reliability of the energy sector has fallen under increasing attention over the last few years due to sophisticated cyber-attacks against critical infrastructure in multiple states. The consequence of such attacks in Australia may not only impact energy organisations, but have broader impacts to society, public health and safety, and our nation's economy.

In response to the increasing threat landscape, Western Power has adopted the Australian Energy Sector Cyber Security Framework (AESCSF) as the maturity framework and related reference frameworks to implement necessary controls to manage cyber risks.

To mitigate these cyber risks Western Power seeks to:

(i) ensure the operation of systems and business information requirements are effectively protected

(ii) evolve the Western Power security profile using a risk-based approach to new practices

(iii) promote continued security awareness amongst all persons making use of its physical and logical assets

(iv) provide Control Owners with the minimum set of cyber security requirements.

1.3 Scope

This Standard applies to all Western Power Personnel.

In this Standard, Personnel means:

(i) Every employee, officer and director of Western Power, and

(ii) Any external service providers or contractors performing activities on behalf of Western Power.

2. Details

2.1 Outcomes

(i) Cyber security is integrated into the organisation's Policies, Frameworks, Standards, Guidelines and Procedures to ensure systems are secured against misuse and attacks.

(ii) Provide a robust and secure operating environment for users and maintain Western Power's reputation.

(iii) Effective compliance with legal and regulatory requirements.

(iv) Accountability for cyber security compliance is embedded at all levels of the organisation.

(v) Provide guidelines and work instructions to support the principles defined in this Standard.

(vi) Appropriate measures and controls are taken to support the operation of systems and applications to ensure Western Power and our customers are protected.

(vii) An organisation with a strong capability of detecting, responding to and recovering from cyber security breaches.

2.2 Principles

2.2.1 Cyber Security Organisation

Objective: To provide a top-down management structure and mechanism for coordinating security activity and supporting the cyber security function.

(i) A cyber security strategy is to define the objectives which are to be in place to meet the overall business strategy and to adopt a risk-based approach

(ii) The cyber security management plan defines the cyber security organisation

(iii) Activities, responsibilities and authorities for roles relevant to cyber security are assigned and documented in the cyber security management plan and then communicated to the organisation

(iv) A cyber security capability skills matrix is to be maintained, and gaps remediated

(v) Training is available to perform the activities related to cyber security roles

(vi) Strong cyber security architecture is established and maintained by means of segregating the data network into risk zones

(vii) Sound and secure system development methodology is established and maintained, which is based upon industry best practices.

2.2.2 Cyber Risk Management

Objective: To ensure key cyber security risks are identified, assessed and treated within the defined limits set by the organisation.

(i) Cyber security risk assessment process is established and maintained which aligns to the Enterprise Risk Management Standard

(ii) Criteria for performing cyber security risk assessments are established

(iii) Analysis of identified cyber security risks is undertaken in a timely manner

(iv) Identification of cyber security risk ownership and their responsibilities are clearly articulated

(v) Cyber security risk treatment plans are established, prioritised and monitored.

2.2.3 Cyber Security Awareness and Training

Objective: To create a culture where expected security behaviour is embedded and where all relevant individuals make effective risk-based decisions and protect critical services and sensitive information used throughout the organisation from being compromised.

(i) Cyber security awareness and training program is established and maintained and aligns to the cyber threat profile

(ii) Employees and contractors shall receive appropriate cyber security awareness and training, aligning to the criticality and risk profile of their job function

(iii) Measures of the effectiveness of training are established including simulation exercises.

2.2.4 Identity and Access Management

Objective: To ensure that only authorised individuals gain access to business applications, information 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.

(i) Identity and Access Management control arrangements are established to restrict access to applications, systems and networks

(ii) The process for provisioning, deprovisioning and changes of identities, credentials and access is established and maintained

(iii) Identities, credentials and access are reviewed at least annually by the information or system owner or delegate

(iv) Additional controls are to be applied to identities, credentials and access with elevated levels of privileges

(v) Enforce a role-based access control model to grant access based upon organisation-defined roles as opposed to positions

(vi) Access is provided on the basis that the user complies with Acceptable Use terms which promote a 'risk-aware' culture of Responsible use

(vii) Access is to be granted with default access and based on the principle of least privilege

(viii) Access privileges should not be assigned collectively (e.g. shared identities) unless special circumstances apply

(ix) Access requests must be approved by the information or system owner or their delegate

(x) Passwords are established and maintained in alignment with the [Western Power Password Management Guideline - to be create].

2.2.5 Logging, Monitoring & Operations

Objective: To help identify threats that may lead to a cyber security incident, maintain the integrity of important security-related information and support forensic investigations.

(i) Important security-related information and events are recorded in logs, stored centrally and protected against unauthorised change

(ii) Identification of systems or devices on which event logging is enabled

(iii) Systems or devices are configured to generate security-related events and event attributes associated with each event

(iv) The retention period of security-related event logs is established and is in alignment with the record keeping plan

(v) Security-related information and event logs are monitored and analysed on a regular basis, using a combination of automated and manual methods

(vi) Detection of anomalous system and network behaviour are established

(vii) Alert and alarm configuration and thresholds are established

(viii) Common Operating Picture is established and maintained.

2.2.6 Threat and Vulnerability Management

Objective: To address vulnerabilities quickly and effectively, reducing the likelihood of them being exploited, which could result in serious security incidents.

(i) A cyber threat intelligence capability is established, supported by an intelligence cycle and analytical tools

(ii) Cyber threat intelligence analysis requirements are established and include the identification, selection and collection of threat information sources

(iii) Analysis of cyber threat intelligence information is conducted to assist in establishing and updating the Western Power Cyber Threat Profile

(iv) Communication plan exists to govern the sharing of relevant cyber threat intelligence information to defined stakeholder groups

(v) Processes are established and maintained for managing technical vulnerabilities in applications, systems, equipment and devices, which include:

a. identifying known technical vulnerabilities

b. defining the frequency of automated or manual scanning for specific, identified technical vulnerabilities

c. defining the priority of the remediation of vulnerabilities

d. testing of remediation controls before implementation where possible

e. defined the roles and responsibilities for the remediation controls.

(vi) The criticality of business applications, systems, equipment and devices are determined to evaluate the criticality of identified technical vulnerabilities.

2.2.7 Incident Management

Objective: To provide the resources required to help resolve cyber security incidents quickly and effectively.

(i) Cyber security incident management is established and maintained which is to include details of identifying, responding, recovering and following up on cyber security incidents

(ii) A cyber security incident management team is in place and their roles and responsibilities are clearly defined and training is provided

(iii) Channels by which cyber security incidents are reported are defined and understood by all users

(iv) Cyber security incidents are recorded within the Western Power Service Management call logging system

(v) Cyber security incidents are categorised and classified according to their severity and type

(vi) Cyber security simulation tests are conducted at least annually to assess the effectiveness of the cyber security incident management framework

(vii) Integration among the incident response plan, business continuity plan and disaster recovery plan are established.

2.2.8 Supplier Management

Objective: To protect applications, systems, networks, computing devices and information when being handled by external suppliers.

(i) Suppliers and third-party partners of information systems, components, and services are identified and prioritised based on their criticality to the operations of Western Power

(ii) Establish and maintain documented processes for managing the cyber security risks associated with external suppliers and are incorporated into the procurement processes

(iii) Confidential and highly confidential information is assessed prior to sharing with suppliers

(iv) Bidding suppliers (both existing and new external suppliers) are evaluated based on their ability to meet the cyber security requirements

(v) Cyber security related risks that may be introduced by a supplier are assessed

(vi) Suppliers are required to share threat information which poses a risk to the operations of Western Power

(vii) Suppliers are required to comply with personnel vetting requirements

(viii) The cyber security performance for the external suppliers are monitored and Western Power has the right to intervene in the management of risk which pose a threat to Western Power

(ix) The cyber security status of suppliers is assessed/validated on a regular basis, using a consistent and approved methodology

(x) Renewal or renegotiation of contracts with suppliers should include verifying cyber security arrangements and proposing revised cyber security terms and conditions

(xi) Western Power will review and audit supplier practices to ensure compliance with our standards and guidelines.

2.2.9 Asset Management

Objective: To ensure assets operate as intended and do not compromise the security of critical or sensitive information and systems.

(i) Asset acquisition (e.g. purchased or leased) will consider cyber security requirements and vulnerabilities

(ii) Type, criticality and classification is captured for cyber enabled assets

(iii) A register of all assets is to be maintained

(iv) Secure configuration baselines are established which are aligned on industry and vendor best practice

(v) Secure configuration baselines are reviewed, tested and kept up to date

(vi) Compliance processes are enabled against assets and the secure configuration baseline

(vii) Assets are configured to prevent tampering and unauthorised access

(viii) Changes to assets are tested, reviewed and applied using a change management process

(ix) Known cyber security asset deficiencies are recorded

(x) Cyber security requirements are defined for use during the asset disposal process

2.2.10 Information Protection

Objective: To protect information in accordance with Western Power standards, ensure information remains available when required, the integrity of information is preserved and protect from unauthorised disclosure of information.

(i) The Western Power information classification is applied to all information across the organisation, regardless of format

(ii) Information is protected in line with its assigned classification level as per the Information Classification Standard.

3. Dictionary

Words in the first column of the following table are defined terms and have the corresponding meaning shown in the second column of the table. Defined terms appear in this document as capitalised.

Defined term	Meaning
Acceptable Use	Specific 'Acceptable Use' Standards apply to the use of all Western Power 'Information Technology Assets' The definition of 'Acceptable Use' is contained primarily within this Standard and is supplemented by 'Guidelines for the Acceptable Use of Western Power 'Information Technology Assets'. 'Computer Users' are required to read, understand and agree to be bound by the Standard and the Guidelines
Accountable	The staff member ultimately answerable for the correct and thorough completion of the advice or communication, and the one who delegates the work to those Responsible. In other words, an Accountable officer approves work that Responsible officer provides
Asset	Something of value to Western Power. Assets include many things, including technology, information, roles performed by personnel, and facilities. For the purposes of this Standard, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the network.
Common Operating Picture	A consolidated view (i.e. "single pane of glass") of the current state of Cyber Security operations within an organisation.
Consulted	Those staff members whose opinions are sought, typically subject matter experts; and with whom there is two-way communication
Control Owners	Control owners have the accountability and authority to ensure the ongoing effectiveness of the cyber security controls in place to manage the Risks.
Cyber Security Incident	An event or chain of events that compromise the confidentiality, integrity or availability of information.
Cyber Security Simulation Testing	The development and use of pre-written test scenarios used to recreate a near to real-life event.
Cyber Threat Intelligence	The collection and analysis of cyber threat information about current and potential attacks that threaten the safety of an organisation or its assets.
Data Network	A system that transfers data between network access point through data switching, system control and interconnection transmission lines.
Framework	A structure of procedures and guidelines and other controls that support the implementation of the stated outcomes of policies in a consistent manner in a specified area.
ICT	Information Communication Technology

Defined term	Meaning
Information	Any information created, collected and analysed or otherwise used by Western Power, regardless of format. Includes but not limited to documents and papers, electronic files or records, electronic data contained within a system, database, information store, or Information Product. For the avoidance of doubt, Information does not include the software or computer programs used to organise or store data, nor the physical assets such as computing equipment or storage media. For the purposes of this Standard, all Information Products are considered Information and fall within this definition.
Information Owner	Responsible for ratifying the security classification of the information and data as they have the knowledge of the use and value to the organisation. This includes all newly created information which is classified at their creation by the information owner. They must communicate the information value and classification when the information is released or provided to another entity. They are responsible for controlling access to this information and must be consulted when other entities wish to extend access authority.
Informed	Those staff members who are kept up-to-date on progress, often only on completion of communication and advice
Policy	High-level, brief, straightforward, statements of principle indicating Western Power's intention and direction, to enable effective decision-making processes.
Process	A Process is a series of steps that are undertaken to deliver a business outcome. It may involve multiple people and decision points.
Process Owner	Person with the accountability and authority to manage the Process and its associated Risks and Controls to ensure the Process achieves its objectives.
Responsible	Those staff members who will do the work to develop the communication or advice under this Standard. There is at least one role with a participation type of Responsible, although others can be delegated to assist in the work required
Risk	the "effect of uncertainty on objectives" (cl. 2.1 ISO 31000:2009)
Role-Based Access Model	A method of restricting access based on a person's role which in turn determines the permissions he or she is granted
Secure Configuration Baselines	A documented set of secure specifications for a system or asset, or a configuration item within a system, that has been formally reviewed and agreed upon at a given point in time, and which should be changed only through change control procedures. The secure configuration baseline is used as a basis for future builds, releases, and/or changes
Standard	Refined statements of principle within a specific area covered by a Policy that assist with the achievement and implementation of the stated outcomes of that Policy.
Threat	Any circumstance or event with the potential to adversely impact operations (including mission, functions, image, or reputation), resources, and other organisations through IT, OT, or communications infrastructure via unauthorized access, destruction, disclosure, modification of information, and/or denial of service
Vulnerability	A cybersecurity vulnerability is a weakness or flaw in IT, OT, or communications systems or devices, system procedures, internal controls, or implementation that could be exploited by a threat source.
Western Power	Electricity Networks Corporation

Defined term	Meaning
Western Power Cyber Threat Profile	It is the result of one or more threat assessments across the range of feasible threats to Western Power, delineating the feasible threats, describing the nature of the threats, and evaluating their severity.

4. Further information

If you have any questions in relation to this Standard please contact either the Cyber Security Manager, Head of Function ICT or the General Counsel.

5. Content owner

Chief Technology Officer

6. Accountabilities

Role	Accountabilities
Chief Technology Officer	Accountable for approving the content of this Standard
Head of ICT Function:	(i) Accountable for: (ii) implementing this Standard (iii) preparing, issuing and maintaining any required supporting documentation (iv) ensuring that people affected by the Standard and its related documents are aware of their responsibilities (v) ongoing education (as necessary) (vi) monitoring compliance with the requirements of the Standard and its related documents (vii) ensuring that appropriate remedial actions are taken if there are compliance breaches monitoring the continuing relevance of the Standard and the currency of its contents
Cyber Security Manager:	(i) Ensuring the embedment of the principles outlined in this standard into applicable functions. (ii) The day-to-day management of Western Power's Cyber Security function (iii) The development, implementation and maintenance of the Cyber Security plan. (iv) Provision of organisation-wide guidance and advice on cyber security (v) Investigation and reporting of all Cyber Security specific incidents (vi) Membership of the Cyber Security Industry Working Group (CSIWG)

7. Review

8. Related documents

Title	EDM reference
Australian Energy Sector Cyber Security Framework (AESCSF)	https://www.aemo.com.au/Electricity/Wholesale-Electricity-Market-WEM/Cyber-Security
Information and Communication Technology Policy	EDM# 54209633
Information and Communication Technology Framework	EDM# 54226522
Western Power Physical Security Strategy	EDM# 44569863
ICT Information Management Standard	EDM# 54226418
ICT Enterprise Architecture Standard	EDM# 54209635
ICT Cyber Security Strategy	EDM# 40853501
ICT Cyber Risk Register	EDM# 47120891
ICT Security Incident Management Plan	EDM# 28324628
ICT Acceptable Use Guidelines	EDM# 54209444
ICT Physical Security Guidelines	EDM# 32714605
ICT Security Access Guidelines	EDM# 41290208
Information Classification Standard	EDM# 34242917
Process Control Assurance Standard	EDM# 41488206
Protective Security Standard	EDM# 41485777

9. Approval history

Version	Approved by	Date of approval	Resolution no.	Notes
1.	Managing Director	22/02/2008		
2.	Managing Director	21/09/2009		
3.	Managing Director	23/12/2009		
4.	General Manager Corporate Services	31/08/2011		
5.	General Council	11/08/2014	#070/2014/BD	At this time the document was named the 'Information and Technology Security Policy'
6.	Chief Financial Officer	03/08/2015	004/2015/BD	Under delegation of the Board
7.	Chief Financial Officer	04/09/2019	N/A	Wet signature

Version	Approved by	Date of approval	Resolution no.	Notes
8.	Chief Technology Officer			New Corporate Template applied. New EDM reference number. Related Documents list updated.

Date of approval :

……

Matt Cheney
Chief Technology Officer