Cyber Security Standard

1. Brief description

This Standard specifies security Standards that protect ICT systems and data from unintended or unauthorized access, damage or destruction.

1.1 Related policies

This Standard is made under and supports the information technology and records management policy (DM#12008675).

1.2 Introduction

The ever increasing reliance on information communication technology and the exponentially rising customer expectation on Western Power's performance have made cyber security a critical business activity. Without adequate cyber security, Western Power exposes itself to both operational and strategic risks which can lead to potentially devastating consequences to the West Australian community.

To mitigate these cyber risks Western Power seeks to:

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

(ii) evolve the ICT security profile using a risk based approach to new ICT practices, partnerships and alliances

(iii) promote continued security awareness amongst all persons accessing Western Power's ICT assets

1.3 Scope

This Standard applies to:

(i) all employees, officers and directors of Western Power

(ii) contractors working within Western Power's workforce

(iii) all of Western Power's business activities and operations

2. Details

2.1 Outcomes

(i) Cyber security is integrated into the organisation's policies, work instructions and practices to ensure ICT systems are secured against misuse and attacks.

(ii) Provide a robust and secure ICT 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 increase user security awareness.

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

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

2.2 Principles

(i) Access to Western Power ICT systems is provided on the basis that the user complies with Acceptable Use terms which promote a 'risk-aware' culture of Responsible use.

(ii) Every ICT system and user will have the least set of privileges necessary to perform their role in order to limit the damage resulted from an accident or error.

(iii) ICT systems will have a security framework appropriate with the level of risk.

(iv) ICT services and applications will be protected by multiple overlapping Security Controls.

(v) Users and ICT practitioners will be educated to support Western Power's security principles in the course of day to day activities.

(vi) Security will be intrinsic to all phases of ICT product delivery to ensure cyber-attack-resilience, limit and contain damage and recover rapidly.

(vii) Data will be secured proportionate to its assigned business information classification level.

(viii) ICT services are to be grouped and segregated according to their assigned trust classification level.

(ix) Commercial, legislative and operational sensitive data will be transmitted securely.

(x) Procured Cloud Services will be ICT security compliant.

(xi) ICT services will be security monitored 24 x 7 with all network traffic scanned for malicious intent or content such as viruses & trojans.

(xii) Access to critical business systems will be logged, recorded and validated.

(xiii) ICT security incidents resulting in breach, significant loss of data or service, will be reported to the appropriate authorities.

(xiv) Physical access to ICT devices, systems, telecommunications networks and data centres are secured in accordance with ICT guidelines.

(xv) ICT security processes will be continuously graded on their level of preparedness using the Capability Maturity Model to ensure their effectiveness.

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
Capability Maturity Model	A maturity model containing structured levels that describe how well the processes can reliably and sustainably produce required outcomes.
Cloud Services	Delivery of computing as a procured service rather than a product with the most common form being over the Internet.
Consulted	Those staff members whose opinions are sought, typically subject matter experts; and with whom there is two-way communication
Informed	Those staff members who are kept up-to-date on progress, often only on completion of communication and advice
ICT	Information Communication Technology
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

Defined term	Meaning
Security Controls	Security Controls are safeguards or countermeasures to avoid, counteract or minimize security risks.
Standard	This Cyber Security Standard
Western Power	Electricity Networks Corporation

4. Further information

If you have any questions in relation to this Standard please contact the ICT Area Manager of Enterprise Architecture, the Head of Function ICT or the General Counsel.

5. Content owner

Head of ICT Function: Accountable for:

(i) implementing this Standard

(ii) preparing, issuing and maintaining any required supporting documentation

(iii) ensuring that people affected by the Standard and its related documents are aware of their responsibilities

(iv) ongoing education (as necessary)

(v) monitoring compliance with the requirements of the Standard and its related documents

(vi) ensuring that appropriate remedial actions are taken if there are compliance breaches

(vii) monitoring the continuing relevance of the Standard and the currency of its contents

General Counsel: Accountable for publishing the approved version of this Standard in Western Power's corporate policies register.

A matrix summarising the respective roles and accountabilities in relation to this Standard is appended to this Standard (appendix 1).

6. Accountabilities

Head of *ICT Function: Accountable for:

(i) implementing this Standard

(ii) preparing, issuing and maintaining any required supporting documentation

(iii) ensuring that people affected by the Standard and its related documents are aware of their responsibilities

(iv) ongoing education (as necessary)

(v) monitoring compliance with the requirements of the *Standard and its related documents

(vi) ensuring that appropriate remedial actions are taken if there are compliance breaches

(vii) monitoring the continuing relevance of the *Standard and the currency of its contents

General Counsel: Accountable for publishing the approved version of this Standard in Western Power's corporate policies register.

A matrix summarising the respective roles and accountabilities in relation to this Standard is appended to this Standard (appendix 1).

7. Review

This Standard will be reviewed and evaluated by the content owner at least once in every three year period taking into account the purpose of the Standard and the outcome of the compliance review.

8. Related documents

Description	DM reference
Information Technology and Records Management Policy	DM#12008675
Information and Communications Technology and Record Management Framework.	DM#12022296
Western Power Confidentiality Agreement	DM#2802455
Enterprise Architecture Standard	DM#7851143
ICT Strategy – Security	DM#10081094
ICT Cyber Risk Register	DM#10999657
ICT Acceptable Use Guidelines	DM#12649841
ICT Security Incident Management Plan	DM#8277381
ICT Physical Security Guidelines	DM#12562446
Information Classification Standard	DM#13457761

9. Approval history

Version	Approved by	Date	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

Date of approval: 03/ 08 / 2015

.....

Guy Chalkley
Chief Financial Officer

Appendix 1

Authority matrix for ICT Cyber Security Standard

Principle	*Responsible*	*Accountable*	*Consulted*	*Informed*
Access to Western Power ICT systems is provided on the basis that the user complies with Acceptable Use values which promote a 'risk-aware' culture of responsible use.	ICT staff Business Partners Customers	HOF ICT	IT Leadership Team customers	ICT staff Business Partners Customers
Every system and user will have the least set of privileges necessary to perform their role …	ICT staff Business Partners Customers	HOF ICT	IT Leadership Team customers	ICT staff Business Partners Customers
ICT systems will have a security framework appropriate with the level of risk.	ICT staff ICT Developers Business Partners	HOF ICT	IT Leadership Team customers	ICT staff Business Partners Customers
ICT services and applications will be protected by multiple overlapping Security Controls.	ICT staff ICT Developers Business Partner	HOF ICT	IT Leadership Team	ICT staff Business Partners Customers
Users and ICT practitioners will be educated to support Western Power's security principles in the course of day to day activities	ICT staff ICT Developers Business Partners Customers	HOF ICT	IT Leadership Team customers	ICT staff Business Partners Customers
Security will be intrinsic to all phases of ICT product delivery to ensure cyber-attack-resilience, limit and contain damage and recover rapidly.	ICT staff Business Partners	HOF ICT	IT Leadership Team customers	ICT staff Business Partners Customers
Data will be secured proportionate to its assigned business information classification level.	ICT staff Business Partners	HOF ICT	Records Management	ICT staff
ICT services are to be grouped and segregated according to their assigned trust classification level.	ICT staff Business Partners	HOF ICT	IT Leadership Team Customers	ICT staff
Commercial, legislative and operational sensitive data will be transmitted securely.	ICT staff	HOF ICT Legal	IT Leadership Team Customers Records Management	ICT Staff
Procured, Cloud Services will be ICT security compliant.	ICT staff	HOF ICT	IT Leadership Team Customers Records Management	ICT Staff Customers
ICT services will be security monitored 24 x 7 with all network traffic scanned for malicious intent or content such as viruses & trojans.	ICT staff Business Partners	HOF ICT	IT Leadership Team	ICT Staff
ICT user access to critical business systems will be logged and recorded	ICT staff Business Partners	HOF ICT	IT Leadership Team Customers	ICT staff Risk & Compliance
ICT security incidents resulting in breach, significant loss of data or service, will be reported to the appropriate authorities	ICT staff Business Partners	HOF ICT	IT Leadership Team Legal Records Management	Federal Authorities Customers

Physical access to ICT devices, systems & data centres is secured in accordance with ICT guidelines.	ICT staff Business Partners	HOF ICT	IT Leadership Team customers	ICT staff
ICT security processes will be continuously graded on their level of preparedness using the Capability Maturity Model to ensure their effectiveness	ICT staff	HOF ICT	IT Leadership Team customers	ICT staff