

This extract from the **Western Power Internet Acceptable Use Policy** is published on the Western Power Internet site to promote the policy content to external companies who may use Western Power's IT facilities. External access is required to allow visibility by companies responding to tenders, to satisfy contract requirements regarding awareness and knowledge of published policies.

Summary of general policy

All Western Power employees and users of Western Power's computer systems are personally responsible for the protection of information and computing assets, particularly in the areas of confidentiality, integrity and availability.

Compliance with this Policy is mandatory and will help to protect important business assets such as information, applications and the supporting infrastructure, and minimise the prospect of fraud and loss.

Purpose

To promote awareness, encourage acceptable use, and discourage the unacceptable use of Western Power's Internet technologies.

Scope - Who does this Policy apply to?

This Policy applies to all computer users, a term that includes employees, business partners, contractors, subcontractors and consultants who utilise Western Power's computer systems to access the Internet. The term Internet includes Internet and World Wide Web (WWW).

Outcomes

The intended outcomes of this Policy are:

1. A culture that supports information technology security and Internet acceptable use principles, as identified below.
2. Computer users who are aware of their obligations in respect to Internet access.
3. Computer users who take responsibility for their actions.
4. A secure Internet environment across Western Power.
5. A reduction in Western Power's exposure to risk by implementing appropriate security controls.

Principles

The following principles apply in relation to Internet access and use:

User Responsibilities

1. All computer users must take responsibility for their actions and must be held personally accountable for the consequences of their actions.
2. All computer users are responsible for adhering to the most current version of this Policy and related policies.
3. Computer users must not be granted access to Western Power's Internet technologies unless and until they have read and agreed to abide by both this Policy and Western Power's prevailing Information Technology Security Policy and Electronic Messaging Policy. Acceptance of these policies is required by Western Power's conditions of employment for staff, contractors and consultants.
4. Computer users are responsible for maintaining personal awareness of Western Power policies. Ignorance of policy does not absolve computer users of responsibility for compliance.
5. Computer users are responsible for any use of their account.
6. Computer users must not share account details or passwords.

Compliance

7. Western Power reserves the right to monitor usage and electronically record compliance and/or breaches of this Policy.
8. Western Power may make Internet access reports available to any Internet user and make the report available to the user's supervisor.
9. Western Power will conduct audits periodically on selected accounts.
10. All Internet access from Western Power's network must be via Western Power's firewall.
11. Computer users must not use the Internet to: access or play games; promote or encourage threatening, harassing, insulting, sexist or racist material; access and/or store pornographic, obscene or suggestive material; or engage in other antisocial behaviour.
12. The use of peer-to-peer protocols, such as Kazaa, BitTorrent, Gnutella and eDonkey, is prohibited.
13. Information accessed must not conflict with Western Power's business objectives.
14. Computer users must avoid excessive Internet browsing and Internet downloads.
15. Computer users must not utilise the Internet for unauthorised advertising, political lobbying, private business or for personal gain.
16. Computer users must promptly report all breaches of information systems security, actual or suspected, to the central Information Systems Security Officer.
17. Violations of this Policy may result in disciplinary action being taken.

18. Computer users should exercise their prudent judgment where issues have not been addressed by this Policy, to determine whether actions are contrary to Western Power's business interests.
19. The CIO (or delegate) must approve any departures from this Policy. These policy departures must be documented and must be available for audit.
20. Computer users must comply with relevant Federal and State Acts and other legal requirements.

Privacy

21. Computer users must not place private or confidential information on the Internet, which could be detrimental to Western Power or individuals, or pass that information to external parties, without the written authority of the CIO (or delegate).
22. Computer users must not reveal personal details of another individual without the prior written permission of the individual concerned.

Illegal Use

23. Computer users must not develop or download programs that harass other users, infiltrate a computer system to maliciously alter the software components of a computer or computer system.
24. Computer users must not knowingly infringe the copyright or other intellectual property rights of Western Power or third parties. You must not download or store items such as mp3's, movies or films.
25. Computer users must not vandalise computer systems.

Personal Use

26. Subject to principles 1 to 25, above, some use of Western Power's Internet systems for incidental personal purposes will be tolerated, though not encouraged, provided such use is kept to a minimum and does not adversely affect the performance or cost of the Internet connection and is not in breach of the rules of this Policy or related policies.

If you are in doubt about a course of action, please consult the IT Security Officer within IT Branch. Log a call through the Response Centre on 9326 5444.

Consequences of unacceptable use policy violations

Failure to comply with the Western Power IT Security Policy extract may lead to suspension and/or termination of access to Western Power systems, referral to law enforcement authorities for criminal prosecution and / or other legal action, including action to recover civil damages and penalties.

Related policies

This Internet Acceptable Use Policy is one of a series of related policies that form part of the conditions of employment by Western Power and obtaining access to Western Power's Internet technologies. The three key policies are Security, Electronic Messaging and Internet Acceptable Use. Other items available internally include:

- The Privacy Act 1988
- The Copyright Act 1968

Note: For information on copyright, please see:

http://www.copyright.org.au/pdf/acc/infosheets_pdf/G010.pdf
and <http://mipi.com.au/>

Standards and Guidelines for Users of Computing and Network Facilities
Australian Standard – Information Security Management– AS17799

- The Western Power Privacy Policy
- The Western Power E-Messaging Policy
- The Western Power Information Technology Security Policy

Need more information?

Please consult the IT Security Officer within IT Branch.

Policy documents are made available externally to allow visibility to companies responding to tenders, and to satisfy contract requirements re awareness and knowledge of published policies.
