PowerWater

Protective Security Management Policy

1   Policy

Power and Water Corporation (PWC) is committed to protecting the security of its people, information and assets by managing security risks proportionately and effectively. The PWC Board, Managers, employees, service providers and contractors integrate sound protective security practices into all aspects of PWC business to ensure a safe and secure operating environment, support effective delivery of business objectives and services, and promote public confidence.

2   Principles

- It is good business to maintain protective security of PWC people, information and physical assets.
- Ultimately, the Power and Water Corporation Board is responsible for security, but all Managers, employees, service providers and contractors contribute to this by taking responsibility for their own safety and security, and the safety and security of others.
- Good security contributes directly to the PWC safety goal of Zero Harm.
- The security of PWC information and assets is planned and managed.
- Access to PWC information is based on the "need to know".
- Access to PWC sites and facilities is based on minimal sufficient access - the "need to go".
- PWC uses a "Security-in-depth" approach, where layers of security measures are applied and combined based on risk and business impact assessments to achieve the right level of security required to protect people, information and assets.
- All security risks, incidents or near hits are reported and investigated, and action is taken to resolve identified issues.
- Regular security training is essential to maintaining a safe and secure workplace.
- Security is a 24 hour commitment.

Approved by:	Draft Prepared by: Beth Moloney Security Project Officer	Issue Date: 11/10/14	Status: Final
John Baskerville Chief Executive	Updated by: Samantha Day-Johnston Executive Manager Security & Emergency Management	D2012/180671	Version:1

3   Explanation

PWC needs to understand, prioritise and manage security risks to prevent harm to official resources and disruption to business objectives. Security is not just a cost of doing business, but enables the proactive management of foreseeable risks that could adversely affect people, information and physical resources and hinder the achievement of business objectives.

PWC's holistic approach to protective security is outlined in the PWC Protective Security Policy Framework. The framework comprises four core policy areas which are described in greater detail in PWC Protective Security Guidelines and supported by procedures and practical tools:

3.1   Protective Security Risk Management
- Security risks are assessed using established PWC risk assessment and reporting processes.
- Business impacts of security risks are assessed in context.
- Risk treatments are reasonable and practical, and fit with the PWC operational environment and business objectives.
- All security incidents are reported and investigated through the PWC Governance, Risk, Audit, Compliance and Event (GRACE) management system.
- Security measures and controls are regularly audited, tested and exercised.

3.2   Personnel Security
- The identity of employees, service providers and contractors is verified, and security vetting is undertaken when required to ensure the security of PWC people, information and assets.
- Security roles and responsibilities are assigned and implemented across PWC.
- PWC job descriptions, service agreements, contracts and work instructions include relevant security responsibilities.
- PWC maintains a culture of security awareness and education.

3.3   Information Security
- Information in all formats, including ICT and SCADA systems and networks, is managed securely and consistently
- Appropriate and effective sharing of official information is facilitated, and controls are consistent with PWC business requirements and legal obligations
- Access to information is based on the "need to know"
- Policy, procedural, technical and practical safeguards limit the potential for loss or misuse of information, or the potential compromise of the confidentiality, integrity and availability of official information.

3.4   Physical Security
- Physical security measures protect the safety and security of people, information, facilities and assets.
- Security business impact and risk assessments are conducted for PWC sites, and reviewed annually or as prescribed in the site security plan, in conjunction with any organisational, operational or environmental change affecting a site or sites.
- The results of a protective security business impact and risk assessment are incorporated early in the process of planning, selecting, designing or modifying PWC work sites and facilities.
- Access to PWC sites and facilities is based on minimal sufficient access to meet business needs, the "need to go" principle.
- Physical security measures are designed to be scaled up or down when required to ensure the capacity to deal with emergency situations.

4   Specific Accountabilities

Role/Job Title	Accountability
PWC Board	Overall accountability for the operation of the Corporation, including security objectives and strategies, security risk management, security investments, security performance and governance.
Chief Executive	Approves the PWC Protective Security Policy Framework Overall accountability for security direction and priorities to meet the expectations of the Board, Shareholder, workforce, customers and the community.
Executive Leadership Team	Endorses the PWC protective security policy, guidelines and procedures. Accountable for capital and operational expenditure to achieve and maintain agreed security outcomes.
General Managers and Senior Executive Managers	Own and manage site security plans and work instructions applicable to sites under their control. Ensure approved PWC protective security requirements are included in the planning and management of facilities under their control. Accountable for protective security to meet legal obligations; business unit objectives; service delivery; and for the security education and awareness of their staff and contractors.
Deputy Chief Executive, Governance and Corporate Services	Own and manage the PWC Protective Security Management Framework, Policies and Guidelines. Approves protective security work instructions, tools, checklists, and product guides. Accountable for the protective security function and its alignment with PWC corporate functions contributing to resilience, including emergency management; safety; risk management; and business continuity management.
Executive Security and Emergency Management Committee (ESEMC)	A sub-committee of the PWC Executive Leadership Team (ELT), ESEMC supports the ELT to improve the Corporation's resilience, enabling it to efficiently and effectively respond to and recover from security, emergency and disaster events. Ensure governance of security and emergency management related matters within PWC.

Protective Security Management Policy

Role/Job Title	Accountability
Executive Manager Security and Emergency Management	Provides specialist protective security advice and support.
	Develop, monitor and review protective security policy and practices.
	Develop and implement security risk assessment, management and reporting procedures.
	Develop and implement a system for the classification and control of the physical security of PWC sites, facilities and assets.
	Develop and deliver a program of protective security awareness and education for PWC employees.
	Develop and deliver a program of protective security audits, testing and exercises for PWC employees and other stakeholders.
Line Managers	Implement protective security policy and practices.
	Accountable for protective security to meet business objectives and service delivery requirements.
All Managers, employees, service providers and contractors	Implement protective security policy and practices.
	Take responsibility for their own safety and security, and the safety and security of others, as well as the security of PWC information and assets.
Chief Procurement Officer	In consultation with Line Managers, develop, monitor and review protective security inclusions in PWC contracts.
Manager, Facilities Services	Ensures approved PWC protective security requirements are included in the planning and management of PWC corporate sites and facilities.
	In consultation with General Managers, manages site security plans and operational security requirements for corporate sites.
Manager, HR	Develops and implements personnel security policy and procedures.
	In consultation with General Managers, accountable for security vetting of employees relevant to job role and function.
Chief Information Officer	Develops and implements information security policy and procedures, including ICT and SCADA security.
Manager, Work Health and Safety	Works in collaboration with the Executive Manager Security and Emergency Management, to ensure that PWC Safety and Security policies and practices are complementary.
Manager, Risk Assurance and Audit	Manage the PWC Risk Management Framework.

Protective Security Management

PWC's governance framework for protective security, including Policy, Guidelines, Procedures and Tools

PWC commitment to good security, aligned with risk management and safety objectives

Current security environment

Protective Security Framework

Protective Security Policy

Security Risk and Threat Assessment and Monitoring

Security Risk Management	Physical Security	Personnel Security	Information Security
•Risk assessment •Risk reporting •Achievable risk treatment •Auditing, testing and exercising of controls	•Security zones •Asset Security Standards •Security Specifications •Security Design Guidelines	•Clearance •Security training •Incident reporting and awareness	•Policy and procedures •System monitoring •SCADA security

Security Awareness and Culture

Security Awareness & Training Program / Security Audit, Testing and Exercise Program

Business Tools

Site Based Security Plans / Security Audit Checklists / Incident reporting / Security contract provisions

Protective Security Assurance

Security risk reviews / Security Audits / Internal & External Security Reporting / Security Exercises