Department of Industry

Policy

Information Security

NUMBER IND-I-197	VERSION 1.0
AUTHORISED BY Deputy Secretary, Finance Strategy & Operations	AUTHORISED DATE 27/6/2016
ISSUED BY Business and Technology Services	EFFECTIVE DATE 30/6/2016

Policy Statement

The department is committed to delivering high level service and satisfaction to its clients. Effective information security management is critical for our organisation and the employees, clients and citizens. This Information Security Policy describes the department's approach to managing the security of information as it pertains to business systems and ICT services. It aims to provide a consistent and integrated approach across all divisions and related entities, and is aligned to the NSW Government Digital Information Security Policy and the NSW ICT Strategy.

Objectives

The key objectives of the policy are to:

- Identify, classify and implement suitable measures to protect the NSW Department of Industry (DoI) information
- Manage and minimise ICT risks
- Manage ICT costs
- Establish an organisational culture that ensures information security management is embedded in activities and business processes, and not as an afterthought or add on
- Build an integrated and agile security capability
- Provide a framework for the governance of information security activities
- Be responsive to changing internal and external threats
- Support consistency in the delivery of DoI services
- Support legal, statutory and contractual compliance

Scope

This policy applies to:

- All employees including contractors, consultants and outsourced service providers performing work for the NSW Department of Industry; employees affected by the policy are referred to as “staff”
- DoI agencies and entities
- All information assets owned by DoI agencies and entities
- Information assets for which DoI have a custodial responsibility. Regardless of whether the assets are on NSW Government property or at other locations, such as third party sites, “cloud” and private residences
- Information in all of its forms, whether printed or handwritten, stored electronically, transported by post or using electronic means. Multimedia in all forms

Requirements

- Information Security Management Framework
    - An Information Security Management System (ISMS) based on the AS/NZS 27001:2013 standard must be implemented by the Office of the Chief Information Officer , providing a risk-based approach to information security management
    - An Information Security Steering Committee must be established to ensure business governance of the ISMS and management commitment to information security principles and activities
    - Agencies and entities using outsourced ICT service providers must ensure that service providers meet business requirements for information security and are subject to baseline security controls and ICT policies
    - Entities using in-house or outsourced significant ICT service provision that are not under management of Finance Strategy & Operations (FSO) must implement an ISMS that

includes business and ICT representatives. The ISMS must be compliant with the AS/NZS 27001:2013 standard or equivalent and may be scaled as appropriate to the organisation

- Policy alignment
    - All information and business systems must be protected in line with the goals of the NSW ICT Strategy, DoI ICT Strategy and the principles highlighted in the NSW Digital Information Security Policy: integrity, availability, confidentiality, compliance and assurance

- Business impact
    - The level of security applied to information, business systems and ICT services must take into account the potential impact of any incident presenting a threat to operation and the cost of risk mitigation

- Risk management and risk assessment
    - Departmental assets and those responsible for them must be identified, and effective, efficient, measurable and proportional controls implemented to mitigate any threats against them, whether threats are internal or external, deliberate, accidental or malicious
    - Information asset and system owners must ensure that an information security risk assessment is completed at appropriate points throughout the business system lifecycle in accordance with the DoI Enterprise risk management framework. Usually these points are establishment, significant change and de-commissioning

- Human resources
    - Information security requirements must be integrated with human resources processes in regards to the recruitment, management and termination of employees
    - Information security requirements must be considered in regards to the engagement of contractors, consultants and outsourced ICT service providers
    - Disciplinary processes must be available to address breaches of this and other ICT policies

- Information classification, handling and labelling
    - All DoI information assets must be classified, handled and labelled according to the NSW Government standards and guidelines, including the DoI Classified information policy

- Identity and access
    - All users of ICT services must be uniquely identifiable and only be granted access to those secured services and information required to perform their roles
    - Duties and responsibilities should be separated in a manner that reduces the possibility of unauthorized or unforeseen abuse of information assets
    - Formal approval processes must be implemented for the granting and revoking of ICT accounts and secured information access
    - Records must be kept of each access-related request and its outcome
    - Periodic review of access rights must be conducted by information and business system owners
    - Physical access controls must be implemented to protect nominated secure areas to an appropriate level based on risk

- Baseline security controls
    - Definitions of business requirements for new systems or enhancements to existing systems must contain security requirements, and where necessary risk assessments
    - ICT service providers, whether internal or outsourced, must implement a level of baseline security controls based on risk assessments and demonstrate alignment and understanding of client's security requirements
    - The management of security controls must be standardised across DoI through a continuous consultation process
    - Internal and external ICT service providers must implement effective:
        - configuration, change and release management processes
        - move, add, change, delete processes

        - patching procedures including identification and remediation of “out of support” and “out of service” software, platforms and devices

- External parties
    - Security requirements, including confidentiality, integrity and availability must be considered, and included in any dealings, engagements and transactions
    - Controls must be implemented to protect intellectual property when dealing with external parties
    - The security of information in transit and information stored by external parties must be given special consideration

- Security incident management
    - An incident management procedure must be established and maintained in order to respond to present threats
    - All incidents must be reviewed in order to prevent future occurrences
    - Notifications concerning a privacy data breach must be ticketed in the service desk, then to internal investigation & response team. The Office of the Australian Information Commissioner will be notified, subject to the level of risk involved and the potential harm to the affected individual(s)
    - Malware breaches that demand ransom to decrypt or prevent publication on the Internet will be rejected

- Business continuity & disaster recovery management
    - Business continuity plans must be considered in line with business expectations, risk and investment
    - Business impact assessments must exist for all significant business systems to ensure that requirements are identified and documented
    - Business continuity plans and/or disaster recovery plans must be tested periodically to ensure they are effective and adequate
    - Disaster recovery plans must exist for infrastructure and every system identified as critical to operation

- Monitoring and reporting
    - Information security activities and controls must be monitored and subject to reporting to ensure on-going effectiveness and relevance to the DoI business areas

- Training and awareness
    - Training and awareness in information security must be provided to help ICT users, administrators and others who handle departmental information to make good decisions and act appropriately
    - Where appropriate broader education and awareness should be undertaken for the users and consumers of ICT technology and business systems (e.g. Virus prevention)

- Compliance
    - All ICT systems and ICT service providers must comply with legislative, statutory, contractual and policy obligations
    - Records management platforms will be complaint with the Information Security Policy

- Independent review
    - Information security management and controls must be subject to periodic independent reviews
    - Internal ISMS audits must be performed by the DoI Audit group or an agreed external party
    - External audits related to certification against the AS/NZS ISO/IEC 27001 standard must be performed by a qualified supplier as required

- Exceptions
    - From time-to-time, exceptions to the controls specified by this and other ICT policies are required to facilitate operational and business requirements. Requests for exceptions must have a justifiable business case documented, following a risk assessment and formal review process. The business case must include any relevant information such

as the reason for the request, a designated owner, a scope, and a timeframe for implementation and termination/expiry
- The Information Security Steering Committee or the Chief Information Officer may approve exceptions
- Exceptions to this policy should be reviewed on a periodic basis

Procedures

Detailed security policies, standards, guidelines and procedures are issued from time to time to support implementation of this policy. These documents will cover specific information types and systems and notify security rules with which staff should comply.

Roles and responsibilities

1. *Deputy Secretary*
   The Deputy Secretary is responsible for:
   - Advocating the implementation of information security principles and practices throughout the NSW Department of Industry
   - Ensuring that adequate and proportionate resources are allocated to securing the information held and used by the NSW Department of Industry according to business requirements
2. *Heads of divisions*
   Heads of divisions are responsible for:
   - Advocating that their staff, consultants, contractors and outsourced service providers, comply with this and other ICT policies
   - Promoting, supporting and facilitating a culture of security within their divisions
3. *The Office of the Chief Information Officer*
   The Office of the Chief Information Officer is responsible for:
   - Administration of this and other DoI ICT policies
   - Leading the introduction, operation, implementation, maintenance and continuous improvement of the information security management framework, associated policies and reports
4. *Staff*
   Staff are responsible for:
   - Complying with this and other ICT policies
   - Using information and business systems only for the purpose intended
   - Exercising due care and diligence for all departmental assets, including when accessing information assets outside of their work location on portable devices
   - Being accountable for all actions performed under their network/system account(s)
   - Protecting departmental information and records from unauthorised or accidental disclosure, modification or loss
   - Reporting information security incidents, breaches of this policy and suspected information security weaknesses
   - Upholding and promoting a culture of awareness and information security

Safety considerations

The safety and security of staff should take precedence over security of departmental information and information assets. Staff should not unreasonably put themselves at risk of injury or harm to protect departmental information or assets.

Delegations

Not listed

Definitions

- Asset: is any tangible or intangible thing or characteristic that has value to an organization. There are many types of assets. Some of these include obvious things like machines, facilities, patents, and software. But the term can also include less obvious things like services, information, and people, and characteristics like reputation and image or skill and knowledge

- Business system: is a combination of people, hardware, software, communication devices, network and data resources that process (can be storing, retrieving, transforming information) data and information for a specific purpose
- ICT' stands for 'Information and Communications Technology'. For the purposes of this policy it includes, but is not limited to, the department's: computers (including desktops, laptops, notebooks and tablets),phones (including landline phones, mobiles and smartphones), software (including email and the Microsoft Office suite), networks, and network connections including the internet, devices for printing, scanning, faxing, copying, and removable storage devices.
- Information asset: includes documents, files and information stored within fileshares, databases, applications systems and services used to create, access, store and transmit this information. Also includes any other representation of this information regardless of medium
- Information security: preservation of confidentiality, integrity and availability of information assets; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
- ISMS: the Information Security Management System is a framework of policies and procedure providing clearly defined practices for the secure management of information and its associated infrastructure
- Malware is any software instructions that were developed with the intention to cause harm, disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising
- The NSW Department of Industry, Skills and Regional Development is known as the NSW Department of Industry (DoI)
- Personal Information: Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics. [Adapted from Privacy and Personal Information Protection Act 1998 (NSW), Part1, s4]
- Privacy data breach: when personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference

Legislation

- Copyright Act 1968 (Commonwealth)
- Crimes Act 1900 (NSW)
- Crimes Act 1914 (Commonwealth)
- Government Information (Public Access) Act No.52 2009
- Government Sector Employment Act 2013
- Independent Commission Against Corruption Act No. 35 1988
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Privacy and Personal Information Protection Act No. 133 1998
- Public Finance and Audit Act 1983
- State Records Act 1998 (NSW)
- Taxation Administration Act No. 97 1996
- Workplace Surveillance Act No. 47 2005

Related policies

- Classified information policy, IND-I-196
- Code of Conduct, IND-P-184
- Conflicts of interests policy, IND-P-183
- Enterprise risk management policy, TI-A-135
- Fraud and corruption prevention policy, IND-P-188
- Gifts and benefits policy, IND-P-189
- Internal Audit and Risk Management Policy for the NSW Public Sector (NSW Treasury, TPP15-03)
- NSW Government Digital Information Security Policy (NSW Office of Finance and Services, OFS-2015-05)
- Records management policy, IND-I-177

Other related documents

- International Standard AS/NZS ISO/IEC 27001:2013
- NSW Government Information Classification and Labelling Guidelines (Department of Finance, Services and Innovation, DFSI-2015-01)

Superseded documents

This policy replaces:

- A-055 Information security

Revision history

Version	Date issued	Notes	By
1.0	15/03/2016	New policy aligned to the NSW Government Digital Information Security Policy and the NSW ICT Strategy	Information Security and Availability Manager

Review date

30/06/2017

Contact

The Office of the Chief Information Officer
Email: security@industry.nsw.gov.au