Secure ICT assets policy

Date approved	May 2022
Review date	February2023
Policy owner	Chief Security Officer
Cohesion link	Secure ICT Assets Policy

Policy overview

1. This policy describes the high-level principles the Department of Internal Affairs (DIA) uses to secure the ICT assets (i.e. systems, services and environments) that it uses to meet its objectives.

Audience and application

2. This policy primarily informs and directs staff responsible for the design, implementation, operation and management of the ICT systems, services and environments that are used by DIA.
3. It is also relevant to designated Business Owners of DIA's information assets, and to project staff who are designing or implementing new ICT services for DIA.
4. This policy applies to:
    - All ICT systems, services and infrastructure used by DIA, whether operated and managed by DIA, our Service Providers and Vendors, or by other third parties (such as cloud services);
    - All DIA groups, branches, affiliates and joint ventures;
    - Every person employed, contracted or engaged by DIA;
    - All ICT assets such as hardware, software, tools and utilities used in the operation and delivery of information technology to DIA.

Delegated authorities and responsibilities

5. The designated Business Owner for each information asset is accountable to the Chief Executive for its security.
6. Technology Services and Solutions (TSS) are delegated with responsibility for the day-to-day security operations and management functions that enable the security of DIA's enterprise ICT assets.
7. Third party providers have delegated responsibility for the day-to-day security operations and management functions that affect the security of DIA's ICT assets, where operational support has been outsourced to them.

8. TSS is responsible for ensuring that project and programme managers are aware of DIA's project security practices, to ensure that development projects adequately address security risks;

9. Project and programme managers are responsible for ensuring that projects comply with this policy when implementing or updating ICT systems and services.

Detailed policy

10. The following principles apply:

Security considerations for the ICT asset lifecycle

11. ICT security is not a single point in time activity or function. Whether an ICT asset is in development, in production or at end-of-life, risks to information security always need to be considered and managed.

12. Information systems and services (including security services) must be managed and maintained throughout their lifecycle, to protect against security threats and known vulnerabilities.

13. The business requirements for information security must be defined and documented for all new ICT services, and for proposed changes to existing ICT services. A risk-based approach must be taken to determine the business requirements for security controls.

14. Information security risks to ICT assets must be identified, assessed and managed to ensure that they remain within the designated Business Owners' risk appetite throughout the asset lifecycle.

15. Use of information from a production environment in other environments must be approved by the designated Business Owner of the information asset. Measures must be taken to adequately protect information outside the production environment, such as ensuring that only necessary information is exported, limiting access to the information in the non-production environment, and purging the information along with verification that the purge is complete once its use is no longer required.

16. Planning, design, acquisition, implementation and operational controls based on a risk assessment must be implemented, to ensure that security is aligned with the business objectives for all ICT assets, and that the security of the ICT environment is not compromised by the introduction of new systems.

17. Protective controls must be in place before new services are implemented in production environments unless all designated Business Owners affected by the new service have formally accepted all risks.

18. Where delivery or support of ICT assets is outsourced, the contract with the outsource provider must specify any requirements and expectations that DIA has for securing the asset and the information it processes.

19. Ongoing support and maintenance controls must be in place and appropriately managed to ensure that ICT assets continue to meet business objectives. Such controls will include:

    a) Asset management, to ensure all assets, and their configurations, are recorded, and their lifecycle managed to ensure they continue to meet business objectives

b) Change management, to ensure that business objectives continue to be met following a change

c) Configuration management, to ensure that the configuration of ICT assets addresses any security vulnerabilities and is defined, assessed, registered and maintained

d) Segregation of environments, to ensure that development, test and production environments are appropriately segregated, and that segregation of duties is enforced across these environments

e) Patch management, to manage the assessment and application of patches to software in order to address known vulnerabilities in a timely manner

f) Service level management, to monitor, manage and align ICT security with business objectives

g) Capacity and performance management, to ensure that the current and projected requirements of the business are met

h) Vendor management, to ensure that security requirements are met by service providers.

20. Decommissioning and destruction controls will be used to ensure that information security is not compromised as assets reach the end of their useful life.

Secure software development

21. ICT security must be considered at all stages of the software development lifecycle, including:

a) During planning and design, ensuring that the right set of security controls is identified and scoped to meet the business requirements for security

b) Security by design, where functional and non-functional security requirements are treated on an equal footing to business and functional requirements

c) Secure development and coding practices, to ensure that common vulnerabilities are avoided, and appropriate code security and quality checks are incorporated into the development process

d) Security testing and vulnerability scanning, via automated and/or manual processes, to identify and address security issues prior to deploying code and systems into production, and on an ongoing basis thereafter.

Standard operating environments

22. All operating systems and applications must be securely configured and managed.

23. Deployment of Standard Operating Environments (SOEs) allows DIA to reduce the time and cost of deploying, configuring, securing, maintaining, supporting and managing ICT assets such as workstations and servers.

24. Where DIA has control over the configuration of operating systems and applications, such as systems that are managed by DIA directly or by our support vendors, SOEs will be used to meet designated Business Owners' functional and security requirements.

25. Where DIA does not have control over the configuration of operating systems and applications, such as for software as a service or other cloud systems, the designated Business Owner must confirm that their security requirements are met through the use of SOEs or other appropriate controls.

26. Business requirements that are unable to be met through the use of SOEs must be appropriately authorised, and alternative compensating controls deployed. It is recognised that business units may have special needs an SOE cannot meet.

27. SOEs must be reviewed on a regular basis and updated as appropriate, to meet changes in business requirements and the external threat environment.

ICT security technology solutions

28. DIA will deploy appropriate ICT technology solutions (such as firewalls, gateways, network access control, intrusion detection and/or prevention, anti-malware, encryption and monitoring and analysis tools) in key locations to control, manage and monitor the security of information and services.

Monitoring, accountability and audit trail

29. Audit logging and monitoring enables information security incidents to be detected and investigated. Without audit logs and monitoring processes, it may not be possible to identify how an incident occurred, recover from the incident, or act to reduce the likelihood of it happening again.

30. ICT systems and applications must be configured to generate audit logs that record user and administrator activities, exceptions and information security events.

31. ICT assets require audit trails that:

    a) Satisfy business requirements (including regulatory and legal);

    b) Support the detection and investigation of security incidents and exceptions;

    c) Facilitate independent audit;

    d) Assist in dispute resolution;

    e) Assist in the provision of forensic evidence if required.

32. Audit trails must be secured to ensure the integrity of the information captured, including to the level required for the preservation of evidence where appropriate. The requirements for the retention of audit trails must be defined by the designated Business Owner.

33. Monitoring and alerting processes must meet the minimum requirements for government and any additional requirements identified by the risk assessment must be in place, to identify events and unusual patterns of behaviour that could impact on the security of ICT assets. Alerts must be investigated in a timely manner through the appropriate incident response process.

34. The designated Business Owners must ensure that users with privileged access rights (such as system administrators) are subject to a greater level of monitoring appropriate to the level of increased risk that they represent.

Incident management

35. All staff must notify the Service Desk of any actual or suspected information security incidents as soon as is practical.

36. To minimise the impact on DIA, appropriate and robust processes must be implemented to respond to and manage information security incidents in a controlled and coordinated manner.

37. Clear accountability must be defined, and communication strategies developed and maintained, to limit the impact of ICT security incidents and facilitate timely resolution. This includes methods for escalation to management.

38. Designated Business Owners must meet their responsibilities to notify external parties of particular types of incident (e.g. in relation to breaches of privacy, identity theft, or human rights breaches).

39. Contracts with providers of outsourced services including cloud services must include requirements for the identification and handling of incidents by the provider and specify how these will integrate with DIA's incident response plans.

Information recovery

40. Appropriate strategies must be designed and implemented for all systems and services to support business continuity and disaster recovery objectives, and to ensure that information assets are not corrupted or lost. This may include the use of data backup and recovery regimes or the replication of data across multiple geographically diverse locations.

41. Information back-ups will be protected using measures proportionate to those in the production system to ensure it is available and to prevent unauthorised access.

Physically secure environment

42. Information and ICT assets must be protected against unauthorised physical access by ensuring that only authorised personnel have access to buildings and secure areas.

43. Based on a risk assessment, environmental controls must be implemented as appropriate to the sensitivity and criticality of the ICT system. The following controls must be considered:

    a) Location and housing that provides a level of protection from natural and man-made threats;

    b) Restricted access to secure areas including procedures for managing access by staff, third party providers and visitors;

    c) Monitoring and alerts for the detection of compromise of environmental controls including: temperature, water, smoke, access sensors/alarms, service availability alerts and access log reviews.

Definitions

44. The following definitions apply when interpreting this policy:

Term	Definition
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.
Availability	The property that information is accessible when required to support business function and operations now and in the future.
Confidentiality	The property that sensitive or private information is protected from unauthorised disclosure.
Designated Business Owner	The individual (role) with accountability for, and the authority to manage, the risk associated with a business information asset (an asset integral to the meeting of business goals and objectives).
Information and Communication Technology (ICT)	The hardware, software, communication and other facilities used to input, store, process, transmit and output information in whatever form.
ICT asset	Any ICT system, service, infrastructure component or environment.
Integrity	The property that information is protected from unauthorised accidental or malicious modification or deletion.
Risk	The effect of uncertainty on the business goals and objectives. The effect can be positive or negative.
Risk appetite	The amount of risk that the designated Business Owner is willing to accept in pursuit of their business goals and objectives. The amount of risk a designated Business Owner can accept is defined by DIA's Risk Management Policy and Framework.
Risk assessment	A process used to identify and evaluate risk and its potential effects. May vary in scope and rigour related to the level of risk. Performed following the DIA Risk Management Framework.
Threat	Anything (eg, object, substance, human) that is capable of acting against an asset in a manner that can result in adverse impacts to availability, confidentiality of integrity.

Related policies, procedures, standards, guidelines, legislation, and/or websites

45. The following documents are relevant to this policy:

- Code of conduct
- ICT access control and management policy
- Digital information protection policy
- Risk management policy