AHPRA Information Security Policy

Purpose and Scope

Purpose

1. This policy provides the organisational direction, management intent and compliance requirements for the security of AHPRA's Information.

2. This policy identifies the information security fundamentals and assigns responsibilities essential to the control of risk when handling information. It contains requirements and guidance for decision making to help ensure that AHPRA meets its legal and regulatory requirements and satisfies its obligations to customers, boards and employees with cost-efficient safeguards.

Scope

3. This policy applies to any person or organisation that accesses, stores or processes AHPRA information assets on behalf of AHPRA. That includes staff members, board members, contracted or temporary staff, consultants, supplier organisations, and partner organisations.

4. This policy addresses various functional areas including business systems, IT operations, application development processes, personnel security, physical security (data centre), legal compliance, business continuity and security management.

5. The policy covers any process, physical or logical storage area that handles or contains information of value to AHPRA.

Information security principles

6. Information security is the preservation of confidentiality, integrity and availability of information. AHPRA's Information Security Policy is based on principals that are central to information security and must be kept in mind at all times when implementing processes, technology and controls.

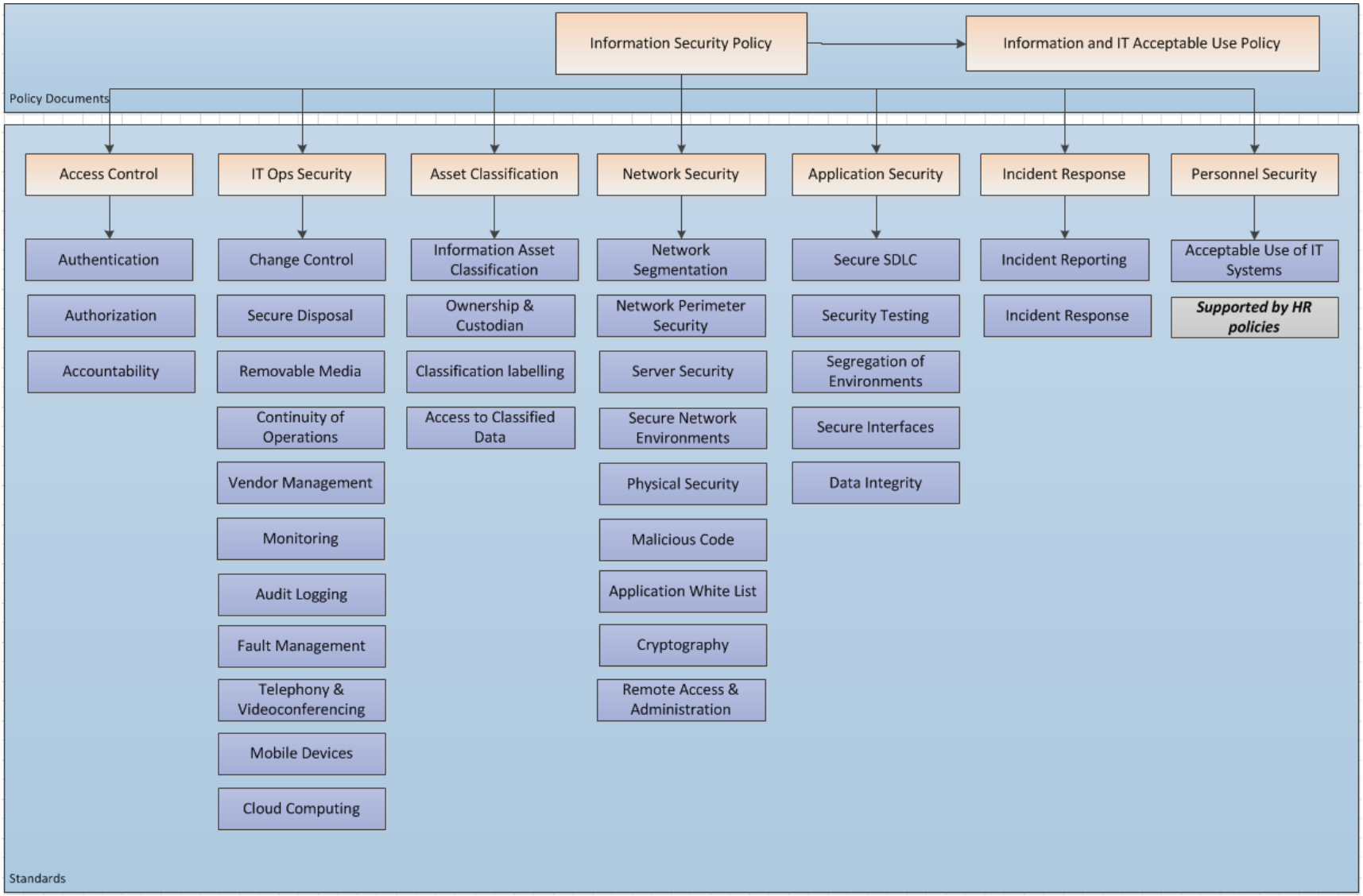
Information Security Principles
AHPRA takes a risk based approach towards information security.
Information must be protected from unauthorised access and unauthorised disclosure. Data must only be accessed on a need-to-know basis.
Information must be protected from unauthorised changes, so it remains factual, accurate and represents business needs.
Information security controls are implemented to ensure that the information remains accessible whenever the business needs it.

Information Security Framework

7. The Information Security Framework provides AHPRA with a structure for policies and supporting documents that outline information security requirements. The Framework consists of key functions that make up the AHPRA IT environment and clearly states the rules that must be followed in order to maintain an appropriate level of security within AHPRA.

8. The policy and supporting standards provide AHPRA's direction and support for information security. Figure 1 depicts AHPRA's security infrastructure.

Figure 1. AHPRA Information Security Policy Hierarchy



Enforcement

9. The Professional Lead Information Technology and Information Security Team has the overall responsibility to promote and enforce compliance of the policy across all functions of AHPRA.

10. All management and staff members are required to be familiar with and comply with this policy within their area of responsibility and their legal delegations.

Non-compliance

11. All users of AHPRA information assets, business functions and systems must comply with the corporate Information Security Policy. Any instances of voluntary non-compliance or breach will be appropriately dealt with by AHPRA.

12. If substantiated, violations of this policy may lead to revocation of system privileges and/or disciplinary action up to and including dismissal.

13. Unlawful activities relating to cyber security will be referred to the appropriate authorities for criminal/civil action.

14. Non-compliance must be immediately reported to the Information Security Team.

Exemptions

15. Exemptions to the policy must be documented and approved in advance by the Information Governance and Assurance Group (IGAG). In order to seek an exemption, a formal request should be made in writing and submitted to the Information Security team. The Information Security team should keep records of exemptions granted and denied.

Audit

16. Compliance with this Information Security Policy will be audited by independent auditors on an annual basis. The scope and schedule of the audit, process followed, audit criteria, findings and responses must be appropriately documented. A review audit must be conducted to ensure response action items are managed and completed. Status of the audits and outcomes must be reported to management on a regular basis.

Policy

Access control

Authentication

17. Users must be uniquely identified and their identity must be validated every time they access AHPRA systems.

18. Suitable authentication methods must be used based on risk exposure. Users must be securely authenticated before accessing information. User credentials must be kept secure.

19. Systems or users accessing AHPRA's secure internal networks from remote untrusted networks must be authenticated by two-factor or cryptographic authentication methods.

20. User access provisioning must follow secure methods when communicating credentials. Identity and password must not be transferred on the same channel at the same time.

Authorisation

21. Access to information must be restricted to authorised users only.

22. Access to information must be authorised based on a 'need-to-know' principle. Individuals must only have access to information, systems or services that are necessary for the proper performance of their duties.

23. IT systems must verify user authorisation levels before granting access to information. Where possible role-based access controls should be used to segregate user access to functionality within the systems.

24. To access any system or data, explicit authorisation must be taken from the information asset owner and there must be audit trails of authorisation given.

Accountability

25. Users are accountable for the actions performed under their allocated login credentials.

26. Access to systems and data stores must be reviewed on a regular basis to ensure appropriate access rights are assigned. Access must be modified or removed in alignment with user's job role changes.

27. Access must be audit logged. Logs must include successful and unsuccessful login attempts. Where appropriate, business transactions performed through systems must be audit logged.

IT operations security

Change control

28. To protect the integrity and availability of the IT and systems environment, all changes must be made in accordance with the change control procedures.

Secure disposal

29. Media containing information that is no longer needed for business purposes must be disposed in a secure manner in compliance with the AHPRA Records Management Policy and AHPRA IT Operations Security Standard.

Removable media

30. Sensitive information stored in portable storage devices and removable media must be protected by authentication and encryption controls.

31. Encrypted removable media containing highly sensitive information must be configured to wipe data automatically if the prescribed limit of authentication attempt is exceeded.

32. Production databases or portions thereof and sensitive AHPRA information must not be downloaded to removable media devices.

33. Information transported outside of AHPRA's secure environments must be must be protected at all times.

Continuity of operations

34. AHPRA must establish and maintain a disaster recovery site capable of meeting business requirements should the primary production site fail.

35. All data and systems required for business functions must be backed up regularly and off-premises copies of backups must be kept. Offsite backup media must be labelled and secured during transport and storage. Restoration testing of random backup media tapes must be performed on quarterly basis.

36. Where business critical systems require high availability, IT systems should be designed to avoid single-point-of-failures within their architectural designs. High availability requirements must be determined by the business needs.

Vendor management

37. AHPRA must have legal agreements with vendors that clearly outline the vendor's security responsibilities for storing or processing AHPRA information and the protection of AHPRA IT facilities.

38. AHPRA shall require vendors with information processing facilities to provide assurance over controls that provide security of information within their operations.

Monitoring

39. Business critical IT systems must be continuously monitored; alerts must be automatically generated. System owners must act accordingly to potential security events. Historical data must be maintained.

Audit logging

40. Audit logging must be enabled at the operating system and application level. Logging must contain sufficient detail to enforce accountability, support investigations and comply with legal requirements.

41. All systems must utilise a central logging store. Audit logs must be protected with tamper proof controls.

42. Audit logs must be reviewed on periodic basis to generate meaningful reports and alerts that will help business goals or to proactively manage the security and availability of production environment.

Fault Management

43. All faults to production systems must be recorded in a central incident management system. Faults must be reported to management. Corrective and preventive action must be managed and monitored till completion.

Telephony and video conferencing

44. Servers and hardware appliances used for the telephony and video conferencing facilities must be securely configured and adequately protected from known vulnerabilities at all times.

45. Access to telephone and video conferencing recordings must be protected from unauthorised access and in accordance with the Access Control Procedure.

Mobile devices

46. AHPRA-issued mobile devices must comply with AHPRA security policies and must be managed by the mobile device management system to enforce security controls.

47. BYO mobile devices used to access AHPRA data and email must be explicitly approved by AHPRA. Such devices must be subject to the same level of security controls as AHPRA issued mobile devices such as the mobile device management system.

48. Any mobile devices accessing AHPRA information must encrypt all data stored within to protect data from loss or theft.

Cloud computing

49. AHPRA's cloud services vendor must provide assurance over their security controls in place to protect the confidentiality, integrity and availability of AHPRA's data and IT environment. The vendor's control policy and practises must be reviewed and approved by the Information Security Manager and the Professional Lead, Information Technology prior to deployment.

50. Cloud computing solutions must be subjected to an information security risk analysis conducted by the Information Security team. Outcomes of the analysis including risks and potential mitigation strategies must be documented. Findings must be reviewed and accepted by the Information Security Manager and Professional Lead Information Technology prior to implementation.

Vulnerability management

51. All AHPRA IT systems must be subject to regular vulnerability assessments. Vulnerabilities and risks must be reported to the management and risks must be mitigated.

52. System software vulnerabilities must be fixed by with vendor supplied security patches as per best practices outlined in AHPRA's IT Patch Management Standard.

Information asset classification and security

Information asset classification

53. AHPRA must classify information assets. The classification model should consider value to business, sensitivity of data and privacy and legal requirements.

Owner and custodian responsibilities

54. System owner and custodian responsibilities must be identified and documented for all of AHPRA's information assets.

55. System owners have the overall responsibility to protect their assigned assets. Owners may delegate the responsibility of implementing specific controls and allocation of adequate resources for the protection of assets to custodians.

Classification labelling

56. To ensure appropriate handling of sensitive and private data, information assets classified as 'sensitive' must be labelled with details of their classification.

Access to classified data

57. AHPRA must implement appropriate user clearance levels to access classified data. Restrictions should be based on clearance levels and must conform to the Access Control Standard.

Network security

Network segmentation

58. Networks must be segmented in zones to secure critical systems, services and data from other less-critical systems. The production environment must be physically or logically segmented from development and test environments.

59. Documentation of security configuration settings must be managed and maintained.

Network perimeter security

60. AHPRA secure environments must be protected with appropriate security controls at the perimeter of the network. Internal trusted and DMZ semi-trusted networks must be protected from unauthorised external access.

61. Firewall configurations must be set to the most restrictive settings. Rules must be reviewed on a regular basis.

62. Perimeter devices must monitor traffic for potential threats to systems within trusted and semi-trusted networks on a regular basis.

63. Electronic data leaving AHPRA's secure networks must be encrypted to minimise the likelihood of data leakage.

64. Data in trusted networks must not be accessible by requests originating from untrusted external networks.

65. Network services providing data services to external parties must be hosted within an appropriately segmented DMZ network. Any changes made to the DMZ network must be subject to information security approval and change control procedures.

66. DMZ services and perimeter devices must be subjected to an annual penetration tests. Network security devices must be subjected to ongoing regular vulnerability testing. The results of these tests must be reviewed by management and appropriate actions taken to address any potential weaknesses identified.

Server security

67. Operating systems, database servers and application servers must be securely configured, regularly monitored for security, and adequately protected from known vulnerabilities and threats at all times.

68. Use of system administration and audit tools capable of circumventing security controls must be documented and strictly limited to authorised IT personnel and adequate audit trails must be available.

Secure network environments

69. IT Operations must provide and maintain secure network environments capable of protecting data and services to meet business requirements.

70. Access to network environments must be restricted to the minimum number of users required to provide adequate support and must adhere to Access Control Standards.

Physical security

71. AHPRA premises must be accessible only to authorised personnel; entry and exit must be recorded.

72. Public access areas must be separated from working areas with the potential of containing sensitive information.

73. Critical systems containing sensitive information must be housed in secure areas which provide environmental controls such as air-conditioning, power management, and fire control. Access must be restricted to authorised staff who have a need-to-know.

74. IT equipment and facilities must be maintained in accordance with manufacturer requirements.

75. All AHPRA IT assets must be labelled for accountability and traceability.

76. All users must keep their desks clear of papers, removable computing devices and removable storage media. Sensitive data stored on any removable media must be kept in a secure area overnight. Privacy screens should be installed where sensitive data could be disclosed to unauthorised persons.

77. Paper records containing sensitive information must be stored in a physically secure area or in locked cabinets. Physical access must be controlled and must be restricted to authorised users who have a need for access.

Anti-Malware

78. Detection and prevention controls to protect against malicious software must be implemented and maintained.

79. Devices without controls against malicious code must be prohibited from connecting to AHPRA's environments.

80. User awareness training relating to threats emerging from malicious code must be undertaken by all AHPRA staff members on a periodic basis.

81. All transmissions into and out of AHPRA must be filtered for malicious code.

82. Systems, devices and removable storage media owned staff and external parties, must be protected against malicious software, prior to connecting to AHPRA networks.

Application white list

83. All AHPRA IT computing devices must be restricted to run authorised applications only. Users must not have the ability to install applications. All devices must be monitored and managed by the IT Service Desk.

Cryptography

84. Where sensitive data is transmitted outside of AHPRA's secure environment, cryptographic controls must be implemented to ensure confidentiality, integrity, authentication and non-repudiation.

85. Cryptographic keys such as private keys and shared secrets must be stored securely; certificates embedded with private keys must be controlled and protected.

Remote access and administration

86. Remote access to AHPRA's internal systems must be authorised. Remote access from public un-trusted networks must be authenticated by two-factor authentication. Data transferred over VPN connections must be encrypted. Passwords, PINs or other authentication tokens must never be transmitted in clear text.

87. Any device connecting to AHPRA's networks must be running software to protect the end users and AHPRA systems against malicious code. Unprotected systems must not be allowed to connect to AHPRA's networks.

Email Security

88. Security controls must be implemented to ensure secure email communication. AHPRA reserves the right to inspect and disclose the contents of electronic mail.

Application security

Secure system development lifecycle

89. Changes to application systems must be made in accordance with the change control procedures and established secure software development lifecycle (SDLC) procedures.

90. Copies of production data must not reside outside of dedicated and controlled AHPRA environments. Data used for development environments must be scrambled or masked to ensure that the data is desensitised.

91. Security requirements must be clearly defined and incorporated into all stages of the SDLC. This is applicable for new systems acquisitions as well as the development or enhancement of existing systems. Security requirements must be reviewed and approved by the Information Security Manager.

92. Source code must be protected to maintain the integrity, confidentiality and copyright of the data. Source code must be version controlled. Coding standards must be established.

93. When implementing a change to existing systems, potential security issues must be documented and reported to the project governance committee. Information security authorisation must be obtained prior to implementation into production.

94. Internet-facing applications should be securely developed based on the Open Web Application Security Project (OWASP) principles and must be subject to independent testing before the change is hosted on the internet.

95. Development must only take place in authorised environments.

Security testing

96. Test plans should include security test cases to identify potential vulnerabilities with functional and non-functional requirements.

97. Access reviews are to ensure that only authorised users have access to shared development environments must be performed every six months.

98. All applicable changes should be tested for performance related issues and security flaws prior to implementation into production.

Segregation of environments

99. All development and test environments must be physically or logically separated from the production environment.

100. Production environments must not be accessible by development team members. Access to production must be restricted to those that are responsible production support.

101. Production data used in sandpit and uncontrolled development environments must be desensitised. Developers must not have edit access to production environments.

102. People with access to the production systems and data within them, must adhere to the Access Control Standards.

103. Duties and areas of responsibility must be segregated in order to avoid collusion and reduce opportunities for unauthorised modification or misuse of information or services.

104. Where segregation is required, controls such as monitoring of activities, audit trails and management supervision must also be implemented.

Secure interfaces

105. IGAG must authorise data interfaces with external organisations.

106. Application interfaces between AHPRA and external organisations must be bound by a formal, signed agreement that states the information security protocols and responsibilities of both parties.

107. Data transmissions must occur over authenticated, secure encrypted channels.

108. AHPRA should use automated, well controlled interfaces when transmitting data between IT systems. Manual transfer of data should be limited to only when cost of automating an interface significantly out weights the risk.

Data integrity

109. Production databases must run data integrity checks on a regular basis.

110. Integrity checks should verify whether AHPRA's data retention complies with PCI-DSS or other applicable regulations.

Incident response

111. Users must report any potential security incidents to the Information Security team. Security incidents must be managed as per AHPRA Security Incident Management standard procedure.

112. Information security incidents must be formally documented.

Personnel security

Human resource security

113. Appropriate background verification checks shall be conducted on employment candidates, contractors and vendors as defined by AHPRA policy.

Compliance

114. All users must comply with all AHPRA policies including the Information Security Policy and the Information and IT Acceptable Use Policy.

Disciplinary action

115. Failure to comply with AHPRA policies may lead to disciplinary action up to and including dismissal.

116. Contract and vendor personnel non-compliance will lead to the cancellation of the contractual agreement and where appropriate, litigation.

Acceptable use

117. AHPRA systems should only be used for business purposes and in the interests of serving AHPRA and its clients.

118. Use of IT systems must be in conformance with the AHPRA Code of Conduct.

119. All staff, board members, contractors and third party users must have knowledge of and adhere to AHPRA's Information Security Policy and Information and IT Acceptable Use Policy. These policies provide detailed directions on usage of AHPRA IT resources.

120. Users must not transmit or store AHPRA information on uncontrolled public internet locations or services.

121. Use of the internet by AHPRA staff is permitted and encouraged where such use supports the goals and objectives of the business. Access to the internet through AHPRA systems is a privilege and all employees are expected to use the internet responsibly and productively.

122. Employees can use the internet for limited personal use provided that this does not impinge on official duties and is conducted in personal time.

Awareness program

123. AHPRA shall provide mandatory information security awareness training to its employees.

124. New employees must satisfactorily complete induction and orientation programs that include information security awareness.

125. When information security awareness training is reviewed and revised, employees must complete refresher training. Training completion must be documented and records maintained.

Vendor and third party personnel

126. Vendor and third party personnel must abide by AHPRA's Information Security and Information and IT Acceptable Use Policies.

127. Third party personnel must be subject to confidentiality or non-disclosure agreements before they are granted access to AHPRA IT systems.

Review and evaluation

128. This policy must be reviewed at least every two years from the date of approval, or when AHPRA goes through a major change that has the potential to change risk exposure.

129. The review must evaluate the policy for suitability, effectiveness, relevance and alignment with business goals.

Related documents

- Information and IT Acceptable Use Policy
- Access Control Procedure
- Application Security Standard
- Cyber and information Security Incident Response Plan
- IT Operations Standard
- IT Patch Management Standard
- Network Security Standard
- Records Management Policy

Definitions

Term	Definition
Business continuity	A predetermined set of instructions or procedures that describe how an organisation's business functions will be sustained during and after a significant disruption of the normal business environment.
BYOD	Bring-Your-Own-Device – Personal or non-AHPRA owned devices used by staff, board members, or external parties to perform their duties or work on AHPRA business.
Cloud computing	A hosted service delivered over the internet. These services can be broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS). For example Office 365, Dropbox
Critical system	An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse or unauthorised access to, or modification of, the information in the application. A breach in a critical application may comprise many individual application programs and hardware, software and telecommunications components. Critical systems can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function.
DMZ	Demilitarised Zone. A network segment managed by AHPRA, but external to the internal corporate production network.
Firewall	A set of related programs that protects the resources of a private network from users from other networks.
Incident	An occurrence that actually or potentially jeopardises the confidentiality, integrity, or availability of an information asset or system that results in violation of security policies, security procedures, or acceptable use policies.
Information asset	Any information or data that is of value to AHPRA that is used to perform business functions.
Mobile devices	Electronic devices that include mass storage as its integral part, such as laptops, smartphones and tablets that could be easily carried away.
Operating system	Software which is designed to control access to services and computer programs installed on a server.

OWASP	Open Web Application Security Project (OWASP) is a worldwide not-for-profit organisation focused on improving the security of web applications. Its mission is to make software security visible, so that individuals and organisations worldwide can make informed decisions about true software security risks. (See www.owasp.org for more details)
System owner	The system owner of information is the AHPRA staff member responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.
Program	A discrete instance of computer program code designed to provide functions or services for a specific purpose.
Removable media	Electronic data storage media that is capable of being removed from the computer or server and could be carried away. Eg. USB, DVD or tapes.
Security control	Safeguards or countermeasures to avoid counteract or minimise security risks. They may be procedural, technical, physical or legal and regulatory or compliance controls
Server	A computer that runs software to provide access to a resource or part of the network and network resources, such as disk storage, printers and network applications. A server can be any type of computer running a network operating system. A server may be a standard PC or it can be a large computer containing multiple drives and a vast amount of memory that will allow the computer to process multiple, concurrent requests.
System	The word system would refer to an information technology system that is defined as a combination of hardware and software components that serves the purpose of information processing. In AHPRA context, this will include all application systems used for core business, HR and Finance support functions
System Development Lifecycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance and ultimately its disposal that instigates another system initiation.
Users	Any person or entity that accesses an AHPRA information asset, by physical or electronic means, either using AHPRA IT systems or their own systems. The term user will refer to staff, contractors, vendor personnel, external agencies, board members and employers.
Vendor	External person, contractor or organisation that provides solutions or services to AHPRA.

Document control

Approver	National Executive
Policy Number	IS002 Version 1.3
Date Approved	13 April 2018
Date Commenced	13 April 2018

Date for Review	April 2021
Policy Sponsor	Executive Director, Business Services
Sections modified	2012 - Updated with feedback from TRAC, Risk Assessment and other standards, CIO, STMC, HR, CEO and Director Finance and Corporate Operations April 2018 – Grammatical and editorial changes, updated links and job titles.