Information and IT Acceptable Use Policy – AHPRA Staff

Purpose

The purpose of this policy is to specify and promote responsible and appropriate use of AHPRA protected information and information technology (IT) facilities managed by AHPRA for the purposes of the National Registration and Accreditation Scheme (NRAS) established under the Health Practitioner Regulation National Law (as in force in each state and territory) (the National Law). This policy is to enable end users to understand the security requirements and policies to be followed for day to day activities.

Introduction

Appropriate and responsible use of AHPRA protected information and IT facilities is use that is consistent with the law and the objectives of AHPRA and the National Boards. It complies with any information security governance arrangements and policies which might be agreed and implemented from time to time.

Scope

The policy applies to all users of AHPRA IT facilities and protected information.

Users are defined as:

• AHPRA employees and contractors who are, or have been exercising functions under NRAS, including staff, consultants and any secondees.

Terms used in this policy are defined in the glossary.

Policy

Using AHPRA protected information

1. Every user handles protected information when performing functions under the NRAS. All users have the responsibility to keep that information secure and use it properly.

2. When handling protected information users are responsible for:

   1.1 conducting themselves in accordance with the National Law, AHPRA Code of Conduct, AHPRA Information Security Policy, AHPRA Privacy Policy and the Privacy Act

   1.2 taking reasonable steps to secure AHPRA data, documents and protected information created in their capacity as AHPRA users. If in doubt staff should refer to the Information Security Policy or consult their manager

   1.3 ensuring the personal information of practitioners is only accessed, modified and/or disclosed where staff are required to do so as part of their official duties. Users must not browse any personal information records that are not directly related to a business transaction they are authorised to perform

   1.4 complying with the security mechanisms built into computing systems and facilities; users must not attempt to circumvent security controls
1.5 securing the login credentials allocated to them and being accountable for activities performed under their login. Users must choose strong passwords and not disclose or share passwords or other authentication material such as access cards and security tokens with anyone.

1.6 not disclosing user or practitioner personal information obtained through their work to anyone for other than for the designated business purposes of AHPRA and only disclosing such information after explicit authorisation or delegation

1.7 not allowing another person to obtain unauthorized access to an information asset by using his/ her right of access

1.8 not using AHPRA IT facilities to improperly store or process information that could result in legal action against AHPRA or the user

1.9 not disclosing any protected information in the public domain without explicit authorisation. Users must refrain from accessing or communicating personal or protected information in public locations (e.g. public transport, transit lounges and coffee shops) unless extra care is taken to minimise the chance of being overheard or having the screen of their device observed, (shoulder surfing).

1.10 keeping desks clear of protected information contained in papers, electronic media and other portable storage media. Documents or portable media containing sensitive data must be kept in a secure area under lock and key.

1.11 not transferring the data, software or documentation to any non-AHPRA party for any purposes other than pre-approved and designated AHPRA business purposes

1.12 ensuring the Information Security Manager is notified of all bulk data transfers and exchanges of significant amounts of protected information between AHPRA and third party organisations, partners or vendors is explicitly approved by the designated authority. The data transfers must occur in designated data communication channels and applied with security controls as required by AHPRA’s Information Security Policy.

1.13 ensuring protected information is not used for commercial gain, advertising, sponsorship, placing a third party in a position of commercial advantage or results in material loss to AHPRA or the boards

1.14 personally download protected information connected with their role in the NRAS and not request, or allow, other people to undertake this task for them

1.15 ensuring that any documents containing sensitive or critical business information are removed from printers and fax machines as soon as possible. Sensitive information must not be sent via fax.

1.16 avoid saving practitioner’s personal information on the desktops and laptops. Ensure to delete it or save it on a designated system once work is completed, and

1.17 ensuring the system is locked (using Alt+Ctrl+Del enter) while users are not present at their system.

**AHPRA IT facilities**

3. AHPRA IT facilities must:

3.1. only be used for business purposes and in the interests of serving the objectives of the NRAS

3.2. be used in conjunction with the requirements of the AHPRA employee code of conduct, policies and guidelines

3.3. not be used in a way that could impact the stability and availability of AHPRA IT systems. This includes, but is not limited to use resulting in performance degradation, tampering with components, reducing the operational readiness of the facilities, wasting or occupying resources.

3.4. not be used to store, transmit, process or view any material that describes or depicts content in a manner that is likely to cause offence to a reasonable adult, and
3.5. not be used for commercial gain, advertising, sponsorship, placing a third party in a position of commercial advantage or results in material loss to AHPRA or the boards.

4. When using the IT facilities, it is the responsibility of all users to:

4.1. respect the integrity of the IT facilities, for example, not to intentionally develop or use programs, data or processes that infiltrate systems or damage or alter the software or hardware components of a system

4.2. not run diagnostics or administrative tools in or against AHPRA IT facilities. This includes but is not limited to connecting any electronic devices to the IT facilities for the purpose of monitoring data, packets, signals and running information gathering tools.

4.3. not install or run programs or other information which could result in the violation of any AHPRA policy or be detrimental to performance or reliability of AHPRA IT systems without preapproval from Information security team.

Using the Internet

3 Use of the internet is permitted and encouraged where it supports AHPRA's goals and the objectives of the NRAS. Access to the internet through AHPRA systems is a privilege and all users are expected to use the internet responsibly and productively. Limited personal internet use is acceptable provided that this does not impinge on official duties and is conducted in personal time.

4 AHPRA has implemented web content filtering to prevent inappropriate and non-business related content and minimise the risk of a security breach. Users may find some websites blocked.

5 AHPRA logs the internet use of all users, these logs can be used for optimising web content filtering policy and investigating reported or suspected misuse.

6 When using the internet, users:

6.1 must not play games, browse offensive content or spend prolonged time browsing websites

6.2 must not view or download entertainment videos in a way that impacts the performance of AHPRA IT facilities or impede professional conduct

6.3 must not upload or store private, sensitive or confidential corporate data in unapproved cloud systems, including but not limited to online data storage sites, document exchange web sites, or personal email accounts. AHPRA does not permit the transmission or storage of any private, sensitive or confidential assets information in a way not endorsed by AHPRA.

6.4 must not post information in internet media, such as social networking sites, blogs or articles that could reflect negatively on AHPRA or its other users, and

6.5 must not download malicious software or applications from the internet and install onto AHPRA IT facilities. Any such need for new software and tools must be requested through the Service Desk portal and provisioned by IT according to the IT provisioning policy.

Using AHPRA email accounts

7 To prevent information security breaches and potential data leakage, documents which are sensitive, private or confidential must only be provided to members of the National Boards and their committees via the designated IT facility, not by email.

8 When using the AHPRA email account, it is the responsibility of all users to:

8.1 respect the intended business use of email exchange and usage shall not be in breach of the AHPRA code of conduct and other corporate policies referred in the 'Related Policies' section of this policy

8.2 report suspected phishing/hoax emails to the Service Desk for further investigation
8.3 be cautious while opening/viewing emails from unknown or suspicious senders. Do not open web links or attachments in SPAM emails. Users should use the ‘block sender function in Outlook to automatically mark email as Junk and move into the ‘Junk E-mail’ folder.

8.4 only send emails to practitioners or members of the public for the purpose of performing their AHPRA or board duties

8.5 avoid emailing protected information of a sensitive, private or confidential nature to external parties. If this is unavoidable, then users are to ensure that the addressee is correct and that the data is properly protected.

8.6 use email only as a correspondence system and do not use email to transfer documents to external parties. Email attachment size is limited to a maximum of 10 MB per email.

8.7 refrain from using AHPRA email addresses in internet forums or for registering in websites not related to job performance or AHPRA or board purposes. Such registrations may result in the user’s email and that of the user’s colleagues’ email being subjected to SPAM and phishing attacks, and

8.8 when accessing AHPRA webmail from the internet and public systems, users must ensure they do not leave copies of attachments with sensitive, private or confidential information in non-AHPRA computers. Any copies made must be deleted after use.

IT equipment & communication facilities

9 When using IT equipment and communication facilities, it is the responsibility of all users to:

9.1 take due care of IT equipment provided by AHPRA to the individual to perform their duties. IT equipment includes mobile phones, tablets, desktops, laptops, security tokens, secure USB drives, wireless internet modems and other computing or media equipment.

9.2 return allocated IT equipment to the Service Desk on the last day of their employment with AHPRA and comply with the Leaving AHPRA Policy or relevant board policies and guidelines.

9.3 ensure personal use is reasonable and appropriate and within specified limits.

9.4 take due care of physical security of AHPRA IT equipment by protecting items from theft or damage at all times. Users must not leave the IT equipment unattended in public places.

9.5 report the loss or theft of any IT equipment to the Service Desk immediately and cooperate with any investigations, and

9.6 sign the conditions of use document provided with an AHPRA iPad.

Monitoring

10 AHPRA may undertake appropriate technical monitoring, recording and auditing of usage of protected information and IT systems as required to comply with legal, technical and policy requirements.

11 In general all activities relating to login, logoff, emails, use of internet, application business transactions, use of document are logged. This logging is required for operational, maintenance, compliance, auditing and security purposes.

12 If at any time there is a reasonable suspicion that AHPRA systems are being used in breach of this policy, the member of the AHPRA National Executive or State and Territory Managers can request that the user’s activities be electronically monitored and activity logs are used for investigation. This will be performed in compliance with legal and regulatory requirements and in compliance with HR policy and procedures or relevant board policies and guidelines.

Using BYO and portable storage devices

13 The use of outside electronic/BYO devices rather than an AHPRA issued device to collect or hold protected information creates a privacy risk for AHPRA. Users must refrain from using BYO devices to access protected information unless explicitly approved. Examples of BYO and portable storage devices include smart phones, tablets, laptops, USB portable storage devices etc.
14 If users have been approved to use a BYO and portable storage devices via the Service Desk Portal, users are required to meet the following requirements:

14.1 BYO devices including smart phones, tablets and laptops that are approved to access protected information will be required to comply with security settings prescribed and enforced by AHPRA. Security requirements will be specified as part of approval process through Service Desk portal.

14.2 Protected information stored in BYO devices must be securely deleted when the device is disposed of or when the information is no longer needed.

14.3 Mobile BYO devices used to access AHPRA email must install Mobile Device Management security software to enforce security controls such as screen password, encryption and ability to remote wipe of containerised corporate data if the device is lost. This is done via a request to the Service Desk portal.

14.4 BYO devices such as laptops to AHPRA must not be connected to internal secure networks (LAN). This means that connecting directly to wall mounted open network ports available in AHPRA offices is prohibited. If any special circumstances require such use, a request must be logged with Service Desk and duly approved by the Information Security Manager, to ensure alignment with security minimum standards.

14.5 Users must not use any unencrypted BYO portable storage devices such as USB drives, thumb drives or detachable hard drives on the AHPRA network.

14.6 Users must only use encrypted portable storage devices, AHPRA issued encrypted secure USB or a similar secure device explicitly approved by the Information Security Manager via the Service Desk portal, and

14.7 The use of portable storage media will be recorded and audited. Users must not transfer data out of the AHPRA network through any other means, including storage in mobile devices such as smart phones.

Remote access

15 AHPRA Anywhere and the other VPN remote access facilities are used to access to the AHPRA network. Remote access is a privilege and must be used in accordance with the AHPRA Flexible Working Policy.

16 The devices used for remote access from must have reasonable levels of security controls as documented in the Working from Home Checklist.

17 Users must be mindful not to leave copies of sensitive and protected information or documents in their personal systems from where they remotely access the AHPRA information.

18 Users must not use public or kiosk computers or computers at transit lounges to remotely connect to the AHPRA network. Users must use secure WebVPN facilities while connecting from free Wi-Fi systems.

Copyright and intellectual property

19 Users must ensure they comply with legislation and contractual obligations relating to the copyright and licensing of programs. Most software on AHPRA IT facilities is licensed by AHPRA from third parties and is protected by copyright and other laws, together with additional contractual agreements.

20 Users must adhere to software licence agreements. Adherence is subject to random audits. Copying of software in a manner that is not consistent with the licence agreement is not permitted.

21 Any intellectual property such as design or architectural documents, process documents, project artefacts, diagrams, analytical reports, software source code created in AHPRA while working for AHPRA belongs to and is a copyright of AHPRA.

22 Users must not install or use freeware applications for commercial use.

Credit card compliance
23 Users must strictly adhere to AHPRA approved credit or debit card handling procedures. Any changes to existing business processes must be consulted and approved by the Information Security Manager.

24 Users must not send or receive credit or debit card information via email, instant messages, chat etc. If a customer offers to send credit or debit card information via email, the user must decline the offer and advise customer to follow the correct process.

25 Credit card information must not be replicated or reproduced. This includes taking photocopies, making notes and keeping unwanted copies of official spreadsheets, documents, either physical or electronic.

26 Users must never ask the customer for CVC/CVV number (the 3 digit number at back of the card) and secret PIN number. This information is not required for AHPRA to process customer payments.

27 Users handling Point of Sale (POS) devices to process credit card information must ensure the POS device is protected from tampering as per the relevant procedure.

28 Users that have access to customer credit card information must ensure the information is used only for the intended business purposes.

29 AHPRA does not re-use customer credit card information for payments. Written consent that complies with AHPRA requirements must be taken from the customer each time prior to processing a payment.

30 Users must ensure physical records containing credit card information is securely stored under lock and key overnight, following the AHPRA clear desk policy. Records must be securely despatched for designated archiving facility when it is no longer needed.

**Reporting non-compliance**

31 Users are responsible for reporting any policy breaches, accidental disclosures, loss or suspicious use of user access credentials, loss of devices, loss of data, incidences of excessive access, security risks, potential information security incidents and threats via the Service Desk Portal.

**Disciplinary action**

32 All users must comply with this Information and IT Acceptable Use Policy. Any instances of non-compliance must be reported via Service Desk portal.

33 Non-compliance or breach may lead to investigation and disciplinary action.

34 Voluntary non-compliance will be dealt with in accordance with HR disciplinary procedures resulting in actions up to, and including, dismissal.

**Related Documents**

- AHPRA Code of Conduct
- Privacy Policy
- Information Security Policy
- Records Management Policy
- AHPRA iPads: conditions of use
- Employee Exit Policy
- AHPRA Flexible Working Policy
- Information and IT Acceptable Use Policy for Board Members
- Any relevant board policies and guidelines
## Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYO device</td>
<td>Means an electronic device a user supplies themselves, rather than a device issued to the user by AHPRA.</td>
</tr>
<tr>
<td>Protected information</td>
<td>Defined under the <em>National Law</em> as:&lt;br&gt;Information that comes to a user’s knowledge in the course of, or because of, the person exercising functions under the National Law.</td>
</tr>
<tr>
<td>IT facilities</td>
<td>IT facilities include, but are not limited to:&lt;br&gt;Hardware such as desktops, laptops, network equipment and communications equipment.&lt;br&gt;Software such as application systems, licensed desktop applications&lt;br&gt;IT services such as internet and email.</td>
</tr>
<tr>
<td>Security tokens</td>
<td>A mobile app, fob or a small electronic device that generates pass codes to gain access to a network or applications.</td>
</tr>
<tr>
<td>Access cards</td>
<td>Proximity ID cards provided to each employee that allow them access to the building.</td>
</tr>
<tr>
<td>SPAM</td>
<td>SPAM is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately.</td>
</tr>
<tr>
<td>Phishing</td>
<td>Phishing is the act of attempting to acquire protected information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.</td>
</tr>
<tr>
<td>Users</td>
<td>AHPRA employees and contractors who are, or have been exercising functions under NRAS, including staff, consultants and secondees.</td>
</tr>
<tr>
<td>Shoulder surfing</td>
<td>The action of someone looking over a user’s shoulder to gather information from the document or a screen that the user is working on.</td>
</tr>
<tr>
<td>Personal Information</td>
<td>Defined under the <em>Privacy Act 1988</em> as:&lt;br&gt;Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.</td>
</tr>
</tbody>
</table>

### Document control

<table>
<thead>
<tr>
<th>Approver</th>
<th>National Executive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>National Executive</td>
</tr>
<tr>
<td><strong>Policy Number</strong></td>
<td>IS001, Version 1.5</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>Date Approved</strong></td>
<td>13 April 2018</td>
</tr>
<tr>
<td><strong>Date Commenced</strong></td>
<td>13 April 2018</td>
</tr>
<tr>
<td><strong>Date for Review</strong></td>
<td>April 2021</td>
</tr>
<tr>
<td><strong>Policy Sponsor</strong></td>
<td>Executive Director, Business Services</td>
</tr>
<tr>
<td><strong>Sections modified</strong></td>
<td>April 2018 – Editorial changes, updated links and job titles, and removal of policy summary</td>
</tr>
</tbody>
</table>