Related procedures
Data Security classification
Password usage
User Registration

It is a condition of usage of Monash Health Information Technology Systems that all employees, affiliates, associates or contractors engaged by Monash Health adhere to the following:

1. Responsibility of users for account security

1.1 Users are responsible for the use of their individual account and must take all reasonable precautions to prevent others from being able to use their account.

1.2 Under no conditions must a user provide his or her password to another person

2. Confidentiality of information

2.1 Users must ensure that the affairs of Monash Health Services, its patients, clients and staff remain strictly confidential and are not divulged to any third party using the computer network except where required for clinical reasons or by law. Such confidentiality shall extend to the commercial and financial interest and activities of Monash Health Services.

2.2 It is the users responsibility to familiarise themselves with the Healthcare Privacy Principles and the Information Privacy Principles.

3. Illegal or destructive activities

3.1 Users will not use the network for any purpose that violates the law or threatens the integrity of the network or individual workstations. For example:

3.1.1 Users will not attempt to gain unauthorised access to the network, or go beyond their authorised access. This includes attempting to log on through another person's account or access another person's files, attempting to obtain passwords, or attempting to remove any existing network security functions.

3.1.2 Users will not actively search for security problems, because this will be construed as an illegal attempt to gain access.

3.1.3 Users will not intentionally develop or use programs to harass other users or to attempt to violate the security or alter software components of any other network, service or system. Examples of such activities include hacking, monitoring or using systems without authorisation, scanning posts, conducting denial-of-service attacks and distributing viruses or other harmful software.

3.1.4 Users will not attempt to damage hardware, software or data belonging to the organisation or other users. This includes adding, altering or deleting files or programs on local or network hard drives and removing or damaging equipment.

3.1.5 Further examples of unacceptable use include, but are not limited to:

3.1.5.1 Fraudulent use of credit card numbers to purchase online merchandise

3.1.5.2 Distributing licensed software or installing software such as games in violation of software license agreements (piracy).

4. Inappropriate material

4.1 Users will not use the network to access or distribute material that is obscene, pornographic, indecent or hateful, that advocates illegal acts or that advocates violence or discrimination toward other people. This includes but is not restricted to distribution through email, newsgroups or web pages. Exceptions may be made if the purpose of such access is to conduct research which the organisation has approved access to.

4.2 If a user inadvertently accesses such information, they must immediately disclose the inadvertent access to the Information Technology Department.

5. Respect for others

5.1 Restrictions against inappropriate language or images apply to personal email, newsgroup postings and material posted on web pages.

5.2 Users will not use obscene, profane, vulgar, inflammatory, threatening or disrespectful language. Users shall not post false or defamatory information about a person or organisation.

5.3 Users will not post information that, if acted upon, could cause damage to individuals or property.

5.4 Users will not harass another person. Harassment is acting in a manner that distresses or annoys another person. This includes, but is not limited to, distribution of unsolicited advertising, chain letters, and email spamming (sending an annoying or unnecessary message to a large number of people).

5.5 Users will not post personal contact information about other people, including address, telephone, home address, work address

5.6 Users will not forward a message that was sent to them privately without permission of the person who sent them the message.

5.7 Users will not send email that does not accurately identify the sender, the sender's return email address, and the email address of origin.

6. Theft of intellectual property

6.1 Users will respect the legal protection provided by copyright law and license agreements related to content, text, music, computer software and any other protected materials.

7. Personal use

7.1 Limited personal use of the Monash Health Services Internet feed is permitted, however, it will be kept to a minimum to ensure that access to business related sites is available at the best possible speed.

8. Violation of this procedure

8.1 In the event there is an allegation that a user has violated this procedure, the user will be provided with a written notice of the alleged violation and an opportunity to present an explanation before an administrator. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the user in gaining the self-discipline necessary to

behave appropriately on a computer network.

8.2 The organisation may at its sole discretion, determine whether a use of the network is a violation of this procedure. Violations of this procedure may result in a demand for immediate removal of offending material, blocked access, suspension or termination of the user's account, or other action appropriate to the violation.

8.3 The organisation reserves the right to act without notice when necessary, as determined by the administration.

8.4 The organisation may involve, and will co-operate with law enforcement officials if criminal activity is suspected.

8.5 Violators may also be subject to civil or criminal liability under applicable law.

Certain violations of this guideline constitute gross misconduct and disciplinary action in relation to violation of this procedure may include dismissal.

Keywords or tags

IT, inappropriate use, Information Technology

Document Management
Policy supported: Information technology security (Operational)
Background: Information technology security
Executive sponsor: Chief Information Technology
Person responsible: Information Technology Security Officer

Declaration

By signing below , I agree to the following terms:

1. I have received and read a copy of the User Responsibilities and understand and agree to the terms of this document in particular but not exclusively noting that;

2. I understand and agree that any computers, software, and storage media provided to me by Monash Health may contain proprietary and confidential information about Monash Health and its patients, clients and suppliers, and that this is and remains property of Monash Health at all times;

3. I agree that I shall not copy, duplicate (except for backup purposes), otherwise disclose, or allow anyone else to copy or duplicate any software installed on any computer under my control;

4. I agree that, if I leave Monash Health for any reason, I shall immediately return to Monash Health the original copies of any and all software, computer materials, or computer equipment that I may have received from Monash Health that is either in my possession or otherwise under my control.

Signature: Subasic

Name: Deva Subasic de Azevedo

Date: 19/3/2025