BEECHWORTH HEALTH SERVICE

Organisational Wide Policy

Org 73 - Information Communication Technology - Network User

Policy Statement

The safety and integrity of Information and Communications systems and the information contained within them is essential for the provision of services and ensuring business continuity can be maintained. Beechworth Health Service will have systems in place to provide this protection.

Applicable to: All staff, volunteers, students and contractors.

Process

SYSTEM ACCESS

- All health service staff will be provided with access to BHS ICT systems in accordance with this policy.
- Executive staff will authorise the applications and privileges for users.
- All users will be provided with an email address
- A new user will only be granted access to the system when the BHS ICT Support or, if they are unavailable, the HRHA Help Desk service.desk@hrha.org.au has received from:
    - Executive Staff- a signed authorisation using the *New User* form **(Appendix 1)** for either a new user or an extension/change of access for an existing user.
    - The user - a signed copy of the BHS ICT user policy form, duly signed by their executive, agreeing to abide by the network policy

Any alterations to existing security levels must be requested by the relevant executive member who will then forward the request to the BHS ICT Support or if they are unavailable, the HRHA Help Desk service.desk@hrha.org.au for actioning, with a copy to the BHS ICT Support.

Logons - A username & password are required to uniquely identify a user to the computer systems and to activate authorised access rights. The user name will be issued by the BHS ICT Support or the HRHA Help Desk.

- From time to time, non - Health Service employees will be granted access to systems as defined by executive staff.
- On completion of a session of use on any computer, users are required to log out of the network and leave the computer in a clean and tidy form ready to be accessed by the next person.
- The user who is logged in remains accountable for the use or misuse of ICT systems under their user name.

PASSWORDS

- The system will force users to change their password on occasions.
- Passwords are to be treated as confidential and as such are not to be shared by any other person or displayed in any public area. Sharing of passwords may result in disciplinary process against the owner of the password and the non-owner user of the password.
- Lost or inoperative passwords will be reinstated by the BHS ICT Support or HRHA Help Desk. Only Executive staff or BHS ICT support can authorise a password to be reinstated.
- Any breaches of security are to be logged as an incident on VHIMS. The HRHA Help Desk may be asked to assist in investigations and to isolate the affected area. Potential viruses or unauthorised access must be treated as a matter of urgency.

CONFIDENTIALITY

- Confidentiality is as per Org 57 Information Privacy and Org55 Codes of Conduct of the Health Service's Organisational Wide Policy Manual.

TERMINATION OF EMPLOYEMENT

- Human Resources is responsible to inform the BHS ICT Support, if unavailable, the HRHA Help Desk service.desk@hrha.org.au of any staff terminations. All privileges and authorised access will be terminated from the end of business hours on the day of termination or as soon as is practical thereafter.

SOFTWARE

- The Health Service in collaboration with HRHA determines the standard suite of software used across Beechworth Health Service ICT systems.
- Software not owned or licenced by the Health Service or HRHA will not be loaded onto the network.
- Software other than the standard suite **must** be evaluated by HRHA prior to being loaded onto any hardware or the network to assess suitability and to ensure that there will be no adverse effect to the network.
- Any documents created by users must be stored in only one location. If the document is relevant to the work of the department then this document must be stored in the Shared Drive for the department which is secure and protected from non-authorised access.
- Only persons who are required to access medical records as part of their employment will have access granted for electronic medical records.
- Under no circumstances are documents to be stored on the local or C drive of a workstation as this jeopardises confidentiality, security and redundancy.
- Users must make every effort to ensure that files or information loaded into the network system (e.g. from email, USB, CD) are not at risk of containing a virus.

EMAIL and INTERNET ACCESS

- All authorised ICT users are given access to email
- Email must not breach any relevant legal and ethical standards and is made available to support staff in their employment.
- Beechworth Health Service Org55 Codes of Conduct applies to the use of email communication.
- Access to the internet is for the purpose of supporting their employment.
- Inappropriate access in working hours for non-work related information may result in disciplinary action.
- The intentional accessing of inappropriate & restricted sites, for example sites containing sexually explicit or pornographic materials are strictly forbidden. The intentional accessing and/or distributing of such materials across the Health Service network are not permitted. Users found to be in contravention of this policy will face disciplinary procedures.
- The user of internet browsing and email services, provided by Beechworth Health Service, will be held accountable for the publishing of any unauthorised and / or inappropriate material. Such actions may also evoke disciplinary procedures.
- The Health Service reserves the right to monitor the use of any user's internet usage.
- The Health Service reserves the right to monitor email exchanges.

PRINTING

- A user shall ensure that any printout from a computer system that contains confidential information remains in their custody until the printout can be disposed of appropriately.
- Printouts must not be left where unauthorised staff can access them.

ADDITIONAL REQUIREMENTS

- If additional software and or hardware other than the Standard Operating Environment of BHS are required, this must be brought to the attention of the unit/department manager.
- The person seeking additional software/hardware will be required to provide documentation explaining the need, the deficit that appears to be present and the solution that they suggest.
- The manager will review the request and if supported they will seek approval from the relevant Executive who will liaise with HRHA and provide them with any specific information they request.

Refer Organisational Wide Policy 126 Information Communication Technology Software Hardware.

Refer Organisational Wide Policy 162 Staff - Mobile Phones and Wireless Communication devices

Refer to HR82 Working from Home Policy V1

Signing this document signifies that you have read and understood the outlined policies and undertake to abide by them.

Applicants Name (Print): ……………………………..

Department: ……………………………

Signed: …………………………………… Dated: ………………………………….

Authorised by:

……………………………………………………………….

Executive member (Director of Clinical Services, Director Excellence & Innovation, Director of Corporate Services, Chief Executive Officer)

………………………………………………………………..

Printed Name

Outcome

BHS will maintain secure and robust ICT systems through the appropriate management of ICT users.

Definitions

HRHA - Hume Region Health Alliance; the entity with overall responsibility for Information and Communications Technology within the Hume health region.

Appendix

Appendix 1 Org 73 Information Communication Technology Network - Appendix 1 New Computer User Request Form

Quality & Risk Management

Goal	Risk	**Rating** (with controls as per this policy)	Required actions

BHS will maintain secure and robust ICT systems through the appropriate management of ICT users	That inappropriate or non-management of ICT users occurs leading to breached security and non-robust ICT systems	Freq= Unlikely
		Conseq = Moderate
		Rating = Medium (6)
			• Specify Management accountability and responsibility
			• Monitor Trends
			• Develop Quality improvement plans

Policy Quality Improvement Action Plan

Specify accountability and responsibility	• Governance and responsibility for this policy is assigned to the Finance Resources and IT Service (FRITS)
Monitor Trends	• Breaches of this policy will be reported and monitored using the Vhims / Riskman incident reporting system • The FRITS Committee will monitor usage of this policy • Annual reviews will be undertaken to ensure 100% of users have stated they have read the policy
Education	• This policy document will be read and signed by all new users. • The Policy will be displayed on the staff intranet • Education will be conducted at staff orientation • Education sessions will be conducted from time to time as deemed necessary
Quality Improvement	Quality Improvement to this policy will be informed at review by: • Feedback (if any) • Department Policy • Industry Guidelines • Incident reports

Document Control

Standards	• National Safety and Quality Health Service Standards Standard 1 Clinical Governance Home Care Common Standards Standard 1 Effective Management • Aged Care: 1.8 Information Systems	
References	• References BHS Organisational wide policies - Privacy, Code of Conduct	
Approving Committees	Finance, Resources & IT Services Committee (FRITS)	Approval Date: 25/05/2021 Approval Date:
Contact Point	Chief Executive Officer	
Review Dates	Issue Date: 20/01/2009 Last Review: 25/05/2021	Next Review: 25/05/2024