Unit 10, 38 First Street, Katherine NT 0851 . PO Box 147, Katherine NT 0851
Phone (08) 8971 9300 Fax (08) 8971 9340
ABN 23 351 866 925 | ICN 3068

Cyber Security Policy

Document Information	
Document Title:	Cyber Security Policy
Version:	PL2024-09-1.0
Category:	Corporate – Information, Technology, and Communications
Approval for use details:	Owner: General Manager Corporate Services Approved by: Senior Leadership Team Endorsed by: Senior Leadership Team Date approved for use: September 2024 Date due for internal review: September 2027
Purpose:	To protect Katherine West Health Board and their clients from cyber threats and data loss.
Related Policies and Procedure/s:	1. Health Promotion iPad Usage Policy and Procedure 2. My Health Record Security and Access Policy 3. ICT Network Outage Procedure 4. Privacy and Confidentiality Policy 5. Social Media Policy
Related Form / Document:	N/A
Key Word/s:	Computers, virus, monitoring, passwords, screen savers, network outage, servers, intranet
External References:	1. Australian Signals Directorate, Information Security Manual Cyber Security Principles 2. Australian Cyber Security Centre, Essential Eight

Background

Katherine West Health Board (KWHB) relies very heavily on having uninterrupted access to Information Communication Technology (ICT) equipment and infrastructure to provide health care and carry out its day-to-day work. KWHB has an electronic operating environment inclusive of electronic medical records, electronic HR records system, email, and various shared files located on servers and an externally hosted data centre. KWHB is committed to ensuring the safety and security of all data.

Unit 10, 38 First Street, Katherine NT 0851 . PO Box 147, Katherine NT 0851
Phone (08) 8971 9300 Fax (08) 8971 9340
ABN 23 351 866 925 | ICN 3068

Scope

This policy applies to the entirety of KWHB ICT environment including desktop and laptop computers, thin clients, mobile devices, printers, networked medical equipment, satellite tracking devices, and peripheral items. It applies to all workers i.e., anyone who carries out work for KWHB including full-time, part-time and casual workers, workers on probation, contract-based workers, self-employed workers, SONT workers, interns, apprentices, students and volunteers. It does not include Board Members or Executive Directors.

Definitions

Term	Definition
Client	Any person using the services of Katherine West Health Board.
Delegate	A person invested with authority to carry out the functions, powers, and duties of, or to act on behalf of or represent others.
Sensitive Information	A special category of personal information that is subject to stricter legal requirements for collection, storage, use and disclosure. Includes health, genetic and biometric information about an individual, as well as information or opinion about the individual's racial or ethnic origin, religious beliefs, political memberships, sexual orientation or practices and criminal record.
Virtual Private Network (VPN)	A secure internet connection that provides private network access to a user while providing protection through data encryption and masking their IP addresses. This also hides their browsing activity, identity, and location, allowing for greater privacy and autonomy.
Workplace	A place where work is carried out for KWHB and includes any place where a worker goes for work e.g., the health centre, a client's home or part of their home, a residential dwelling that is not their home, a vehicle, or a community venue.

Policy Statement

Katherine West Health Board (KWHB) is committed to maintaining a robust cyber security framework to protect the organisation, workers, and the community we serve from cyber threats, data loss and risks to provision of health care services.

The requirements outlined in this document represent a minimum standard that will be accepted by KWHB for all workers when accessing KWHB ICT resources and using the ICT system.

Unit 10, 38 First Street, Katherine NT 0851 . PO Box 147, Katherine NT 0851
Phone (08) 8971 9300 Fax (08) 8971 9340
ABN 23 351 866 925 | ICN 3068

KWHB employs a continual improvement approach to cyber security in line with the Australian Cyber Security Centre, Essential Eight and Australian Signals Directorate, Cyber Security Principles.

Principles

1. Data Security – to protect KWHB client and organisational data from loss or malicious attack.
2. Continual Improvement – for data security measures to remain effective, current, and relevant in a changing environment.
3. Confidentiality - Ensuring that information is not disclosed to unauthorised entities.
4. Integrity - Ensuring that information remains complete, accurate, and protected from corruption.
5. Availability - Ensuring that authorised users have timely access to information when needed.

Responsibilities

The Board will

- Oversee the KWHB ICT system including reports of the effectiveness of the cyber security framework.

The CEO will

- Ensure that a robust cyber security framework is resourced, implemented, and maintained in accordance with this policy, to protect the KWHB ICT system.

All workers will

- All staff are responsible for adhering to requirements of this policy and reporting any suspected cyber security risks or policy breaches to the ICT Service Desk or the General Manager Corporate Services.

Legal Considerations

KWHB must comply with the laws and policies as outlined in the funding agreement between KWHB, the Department of Health and Aging, and the Department of Health, including

- Crimes Act 1914 (Cth)
- Criminal Code Act 1995 (Cth)
- Anti-Discrimination Act 1992 (NT) and Regulations 1994
- Ombudsmen Act 2009 (NT)
- Privacy Act 1998 (Cth) and related Australian Privacy Principles 2014
- Information Act 2002 (NT)

- My Health Records Act 2012 (Cth)
- My Health Records Rule 2016 (Cth)
- My Health Records Regulation 2012 (Cth)

Acceptable Use of ICT Resources

Physical Security

- Users of KWHB ICT resources will maintain appropriate physical security over devices that are within their control to minimise the risk of loss of assets or data.
- If devices are used in locations where the public may be present, care must be taken to prevent information being seen by unauthorised people. Devices must not be left unlocked if unattended for any period and should be shut down or restarted at the end of each day.
- Public WiFi networks should not be used for connecting KWHB devices.
- Approval of the CEO is required before taking any device containing KWHB data outside of Australia.

Loss of equipment

If a user suspects that a KWHB device, or any device containing KWHB data is lost or stolen it must be reported immediately to the Manager Assets and the General Manager Corporate Services. If the device is suspected as stolen it must also be reported to NT Police and the Police report number provided to Assets.

System and Software Updates

Updates to ICT systems and software are managed by the contracted ICT service providers. Users are not permitted to prevent updates or modify security settings in any way. Any additional software that is required for a device must be approved prior to installation and be maintained in line with the vendor's recommendations.

ICT System Monitoring

KWHB and its ICT service providers utilises a range of monitoring products to maintain the security of the ICT environment and enable reporting on security, performance, and usage. These products capture a range of data relating to environment performance, throughput, internet activity, email traffic and content as well as system access and usage by individuals.

Information including users' name; any sites visited; any email messages sent or received; any information posted to sites; and any other records of worker's usage may be accessed at the request of the CEO and may be passed on to someone else for the purposes of meeting an obligation under the laws and policies KWHB must comply with as outlined in the

funding agreement between KWHB, the Department of Health and Aging, and the Department of Health.

Password Requirements

- Passwords created for access to KWHB ICT systems should be unique and contain a mix of upper case, lower case, numbers, and special characters. Minimum requirements for passwords for KWHB systems access will be set by the ICT service provider.
- Passwords should be updated regularly and never shared with anybody. Do not provide any passwords to colleagues, help desk staff or any other party.
- Users are not permitted to allow any other person to access the KWHB network through their log in details. If you suspect that any password is known to anyone else, it must be updated immediately.
- Passwords may be managed through a secure password management tool such as Microsoft Wallet.
- Multi factor authentication (MFA) is a process where a second means of identification such as biometric data or an additional code sent to an email account or mobile phone is required to complete sign in. MFA is an effective means of preventing unauthorised access to systems and accounts. Wherever MFA is available, users are encouraged to have it set up. Some KWHB systems will require MFA to be set up before use.
- Mobile devices that contain KWHB data, including personal devices, must have current security patches/software updates maintained and be protected by passcode and/or biometric security measures.

Email Security

- Each KWHB staff member will be issued with a @kwhb.com.au official email address. All official emails should be sent using an official KWHB email account. Staff are not permitted to use official email accounts for conducting private business or subscribing to personal subscriptions, RSS feeds or any private online services including social media accounts.
- There are risks with emailing client and health information to other healthcare providers and reasonable steps must be taken to protect this information. In person, phone, and SMS are more secure methods.
- Always obtain and record consent from the client before emailing.
- Verify the email address by sending a test email and avoid generic inboxes.
- Sending of sensitive information should be done through secure messaging services wherever possible, such as in Communicare using Argus, Health Link or MQ Link. If email must be used, encryption should be applied, and client consent given.
- Use the BCC field for group emails so recipients can’t see other recipients’ names or email addresses.
- The secure transfer of confidential information is the responsibility of the sender.

Unit 10, 38 First Street, Katherine NT 0851 . PO Box 147, Katherine NT 0851
Phone (08) 8971 9300 Fax (08) 8971 9340
ABN 23 351 866 925 | ICN 3068

- Spam and scam emails are common and KWHB utilises email filtering that minimises the amount of scam/spam emails that are delivered. Some unwanted mail may still be delivered, and staff need to be aware of potential risks. Any suspicious or scam emails that are identified should be referred to the ICT service centre for action.

Data Security

- All KWHB data is stored within secure data centres within Australia, and regularly backed-up. No data is permitted to be backed-up or accessed from any international locations.
- KWHB data must not be stored on laptops, desktops, external hard drives, or portable storage such as flash drives or USB sticks. Data must only be stored in line with KWHB data storage guidelines. Refer to the Acceptable Use ICT Policy for more information.
- Access to KWHB data may be granted though a virtual private network (VPN) connection. VPN access must only be provided to staff/contractors who require the access to carry out their role. VPN access must not be granted to shared user accounts without prior written approval of the CEO or General Manager Corporate Services.
- VPN accounts will be regularly reviewed and may be revoked at the discretion of the CEO or General Manager Corporate Services.
- If there is a requirement to share KWHB data externally e.g., with contractors, vendors or the public, appropriate measures must be put in place to ensure only the required data is shared and that all access is removed when no longer required. Approval must be provided by the CEO or General Manager prior to providing external party access to any sensitive information or network access.
- Any non-work-related data saved and stored on KWHB's ICT network is done so at the worker's own risk. Katherine West Health Board reserves the right to delete any material stored on a Katherine West computer at any time including during maintenance and without notice. Katherine West Health Board accepts no liability resulting from the loss of such material.

Anti-Virus/Malware Protection

The KWHB environment is protected by a range of anti-virus, malware protections and other security products which are implemented and managed through the ICT Service contracts. Users are not permitted to tamper with, disable, delete, any security software/systems on any KWHB ICT assets.

Incident Response

If it is suspected that any data has been accessed by an unauthorised user, leaked to the public intentionally or in error or if a cyber-attack is suspected, the CEO or the General Manager Corporate Services must be informed immediately. Incidents should be recorded in KWHB's incident management system (Donesafe).

The CEO will coordinate appropriate response with the General Manager Corporate Services, ICT service providers and NT Police as necessary.

Unit 10, 38 First Street, Katherine NT 0851 . PO Box 147, Katherine NT 0851
Phone (08) 8971 9300 Fax (08) 8971 9340
ABN 23 351 866 925 | ICN 3068

Access to Systems

- KWHB adopts “minimum required access” and “role-based access” approaches to system and data access. Administrator or elevated access to systems or devices is not permitted without CEO or General Manager Corporate Services approval. All system access is subject to review and may be revoked or downgraded at the discretion of the CEO. Refer to the My Health Record Security and Access Policy for more information.
- Access to clinical systems will only be provided to a worker who has a business need for access, and the minimum required access will be provided.
- System access is allocated to users on commencement based on the role of the worker. Additional access requests require the approval of a line manager and/or system owner.
- Access to systems will be reviewed in the event of a worker changing roles or duties.
- All system access will be disabled if employment is finalised.
- All system access will be disabled during periods of unpaid leave, unless written approval to maintain access is provided by the General Manager and approved by the CEO.

Document Modification History:	1. Creation of Cyber Security Policy to replace Firewalls, ICT Network Access, ICT Access Roles and Responsibilities, Password, Antivirus Management, Disaster Back Up and Disaster Recovery, and Screensavers Policies September 2024

**Any printed or saved documents from the document library may not be reflective of the current version. Check the document library for the most current version.*