POLICY	**Information Communications Technology & Cyber Security**		
DOCUMENT REF	**PS ICT-CS 01**	**EFFECTIVE DATE**	**22 August 2024**
RESPONSIBILITY	**Board / EO**	**REVISION NO.**	**Version 2**

Purpose and Scope

The Hut relies on technology to collect, store, and manage its information.

Human errors, hacker attacks and system malfunctions could cause great financial and personal damage and can easily jeopardise The Hut's reputation.

This ICT & Cyber Security Policy outlines our guidelines and provisions for preserving the integrity of The Hut's and its peoples' data and ICT infrastructure.

This policy applies to all Hut staff, workers, and anyone else who have permanent or temporary access to The Hut's online information and systems and anyone who provides any information to us.

Definitions

Cyber Security	The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
Cyber Resilience	Ability to defend, adapt respond and recover from cyber threats and cyber incidents while maintaining continuous business operations
Cyber Incident	An unauthorised cyber security event, or a series of such events, that has the potential to compromise business operations
Staff	Paid employees and volunteers.
Workers	Any person who works, in any capacity, in or as part of The Hut

Background

The Hut relies heavily on ICT for the storing of both personal and program information, data collection, as a communications tool and reporting. The Hut also depends heavily on the use of social media and its website, for disseminating information about programs and services.

Information is an asset that is critical to The Hut's service delivery and operations therefore, all information that is captured, stored, processed, and delivered by The Hut, regardless of form or format, must be protected proportionate to its value and risk.

The Hut, at various times and when there is a purpose to do so, will collect and store personal and/or confidential information. This information includes staff and participants' name and contact details, date of birth and details about clearances (NPC and Working with Children/Vulnerable People), details of partners and clients and, where there is a need, banking details. This information is collected in line with our Privacy Policy. If not stored correctly, with appropriate security processes and measures in place, access to this information could be obtained or used illegally and subsequent harm could be caused to individuals or the organisation.

Objective

The objective of this Policy and all associated procedures is to provide a framework for appropriate safeguarding measures that will ensure The Hut has maximum security in place to protect it from cyber risks and ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

Policy

Cyber threats are part of The Hut's risk landscape, particularly as we place more key assets and systems in internet facing systems which is susceptible to attacks. The Hut needs to remain responsive to the threat and be resilient to cyber-attacks.

The Hut will: -

- **Avoid** - cyber risk through ceasing or eliminating certain activities e.g. avoiding the collection and storage of unnecessary data
- **Mitigate** – reducing risks by implementing internal processes e.g. Implementing multi-factor password authentication, ensuring patching and anti-virus software is up to date and awareness education for all staff. Due to having limited internal expertise we will also utilise external service providers to maintain the integrity and security of our systems and hardware.
- **Transfer** – Transfer data securely and avoid transferring sensitive data
- Consider **Outsourcing** systems and functions to third party providers may alleviate The Hut having specific IT infrastructure and systems.

Protect personal and Hut devices

The Hut is committed to ensuring staff and workers have access to ICT infrastructure, tools, training, and support that assists them to do their work efficiently and effectively.

All staff are required to keep both their personal (if connected to hut services) and Hut issued computers, tablets and mobile phones secure by:

- ensuring all devices are password protected
- using multi-factor authentication, face, voice or fingerprint recognition technology where available.
- installing antivirus software
- ensuring the device is not left unattended.
- only accessing secure Wi-Fi networks and never using a public Wi-Fi network
- installing browser and systems updates monthly or as soon as notification of updates are received.

New employees will receive instruction on how to protect their devices and refer to either the Hut's Executive Officer (EO) or The Hut's Community Development Manager (CDM) if they have any questions.

Emails

To avoid virus or malware infecting our systems and devices, all employees are advised to:

- scrutinise any received emails for signs of discrepancies or inconsistencies that might indicate a potential threat, including
  - the misspelling of names, use of incorrect grammar or spelling
  - unusual email addresses or website information,
  - a request for urgent attention or action
  - an unusual request from someone whose name you recognise or is in your contacts list. Always contact that person by phone to check its credibility.
- avoid opening attachments and clicking on links when the content is not adequately explained or something you weren't expecting to receive

Passwords

Details of Hut accounts that have shared access across one or more staff or those that hold Hut data or Hut IP, and their associated passwords, will be shared with, and kept secure by, the Executive Officer and Community Development Manager to ensure ongoing access.

To help keep individual passwords secure, all staff will :

- except for the previous paragraph, not share their passwords or log in details with others.
- choose passwords with at least eight characters (including at least one capital letter, one number and one symbol) and avoid information that can be easily guessed (e.g. birthdates) or consecutive numbers
- where possible, use a passphrase rather than password
- Change passwords regularly
- aim to remember passwords/passphrases instead of writing them down. If passwords need to be written, keep confidential and consider writing them in code.

Files will be saved in access restricted Drives and stored on an external server located in Australia or country where data integrity is equal to or higher than in Australia or on the Cloud and managed by a reputable IT management company. Appropriate anti virus software will be installed on all computers with a separate antivirus on cloud drives and storage. Back-ups of data are to be done daily.

Access levels to Hut data and software applications will follow the principle of "need to know", i.e. only the minimum level of access to perform staff duties is granted. To protect information, a system of controlled permissions, passwords and privileges safeguarding access to the shared drive, files and media platforms will be maintained by the Executive Officer.

All use of social media, internet, shared drives, and The Hut's website will be used in accord with The Hut Code of Conduct and Privacy Policy and DHS and NPC screening and training for staff will be undertaken where required, according to roles and responsibilities.

Publicly accessible computers will be divorced from The Hut's administration and network system. All publicly accessible computers will be updated and cleaned regularly with history checked to ensure compliance with terms of use.

Cyber security requirements will be included as part of The Hut's business resilience planning and incorporated into business continuity and service recovery procedures.

Our staff nor any member of the public using our computers mustn't use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

Responsibility

The Board is responsible for reviewing this Policy and ensuring all procedures and systems relating to the Board and its sub-committee are adhered to.

The Executive Officer is responsible to enact this policy.

Related Documents	*ICT – Usage and Security Procedures* *Privacy Policy* *Delegation of Authority* *Hut Code of Conduct*
Legislation & References	Copyright Act 1968 Privacy Act 1988

Signed on behalf of Hut Board by Hut Chair:

Name: David Rawnsley

Signed: Date:

Date Approved by Board: August 2024	Next Review Date: August 2027
