Central Tablelands Water

Information Technology Security and Usage Policy

DOCUMENT CONTROL

Document Title	Information Technology Security and Usage Policy
Policy Number	CTW-PR040
Responsible Officer	Director Finance and Corporate Services
Reviewed by	Council
Date Adopted	14 October 2020
Adopted by	Council
Review Due Date	October 2021
Revision Number	1

Previous Versions	Date	Description of Amendments	Author	Review/ Sign Off	Minute No: (if relevant)
					20/094

Objective

The purpose of this policy is to outline the acceptable use of computer equipment at Central Tablelands Water (CTW) and rules around security access to network resources. These rules are in place to protect the employees and CTW. Inappropriate use exposes CTW to risks including virus attacks, compromise of network systems and services and legal issues.

Definitions

Word/Term	Definition
Information Technology Security	The practice of defending computing devices, networks, and stored data from unauthorised access, use, disclosure, disruption, modification or destruction
Cyber Security Team	Capability appointed by the General Manager. Their responsibilities are outlined in the Cyber Security Policy
CTW facilities and services	Information Technology facilities operated by or on behalf of CTW. This includes services and systems and associated computing hardware and software used for the communication, processing and storage of information
CTW	Central Tablelands Water and controlled entities
CTW Network	The network infrastructure used by CTW including all network service on and off site with trusted access to CTW services
User	Any person using any of the IT facilities and services

Scope

This policy applies to all employees, contractors, consultants and other workers at CTW including all third party affiliates. All users should be aware of this policy, their responsibilities and legal obligations and are required to comply with the policy and are bound by law to observe statutory legislation.

Internet/Intranet related systems, including but not limited to computer equipment, software operating systems, storage media, network accounts providing email, Web-browsing is the property of CTW. These systems are to be used for business purposes in serving the interests of CTW, our customers and the community in the course of normal operations.

While CTW's network aims to provide a reasonable level of privacy, users should be aware that the data created on the corporate system remains the property of CTW.

For security and network maintenance purposes, authorised individuals within CTW may monitor equipment, systems and network traffic at any time.

Principles

All CTW IT facilities and services will be protected by effective management of Information Technology Security risks.

Use of CTW IT facilities and services must comply with CTW policies and relevant legislation. Examples of legal regulation include privacy, copyright, government information (public access), equal employment opportunity, intellectual property and workplace health and safety.

Policy Responsibilities

General Manager, CTW

1. The General Manager of CTW has the following responsibilities:
   a. Taking carriage of CTW's Information Technology Security Policy and supporting framework;
   b. Ensuring effectiveness of Information Technology Security measures through monitoring programs;
   c. Ensuring effectiveness of disaster recovery plans through a program of testing;
   d. Appointing an Information Technology Security team;
   e. Approving complementary operational procedures to support this policy;
   f. Approving the isolation or disconnection of any equipment or IT facility from CTW's network which poses a severe and unacceptable risk; and
   g. Reporting to appropriate governance bodies including the Risk, Audit and Compliance Committee on matters pertaining to Information Technology Security.

Information Technology Security Team

2. The Information Technology Security Team has the following responsibilities:
   a. Owning and operating processes required by the Information Technology Security policies and framework;
   b. Undertaking continuous development and improvement of cyber defences;
   c. Undertaking continuous monitoring and review of practices and defences; and
   d. Conducting education activities to ensure awareness of cyber security threats and defences.

Risk, Audit and Improvement Committee

3. The Risk, Audit and Improvement Committee has the following responsibilities:
   a. Monitoring Information Technology security risks and controls by reviewing the outcomes of cyber risk management processes and monitoring emerging risks; and
   b. Overseeing the adequacy of cyber security capability and controls.

Staff with responsibility for managing any IT facility

4. Staff whom manage any IT facility have the following responsibilities:
   a. Developing, operating and managing the IT facility according to CTW's Information Technology Security policies;
   b. Regularly monitoring and assessing the related Information Technology security controls to ensure ongoing effectiveness; and
   c. Immediately reporting all security incidents and breaches to the Information Technology Security team.

Users of IT facilities and services

5. Individual users have the following responsibilities:
   a. Using IT facilities and services according to IT policies at all times;
   b. Being aware of the security requirements of the IT facilities and services they use, and take every precaution to safeguard their access to these systems against unauthorised use; and
   c. Immediately report any known or suspected security incidents and breaches to the General Manager.

Password Security

Authorised users are responsible for the security of their passwords and accounts and can be held responsible for activities performed with user's credentials.
The following password security rules shall apply:

Account Policies/Password Policy	
Enforce password history	12 unique passwords remembered
Maximum password age	90 days
Minimum password age	1 day
Minimum password length	12 characters, include uppercase letters, lowercase letters, numbers, and/or special characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption	Disabled

Account Policies/Account Lockout Policy	
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

Passwords are not to be shared with other staff. Should a staff member act in your role, then appropriate access will be granted for the duration of the acting period.

Unacceptable Use

Under no circumstances is an employee of CTW authorised to engage in any activity that is illegal under State or Federal legislation while utilising CTW-owned resources. The list below is by no means exhaustive but is intended to provide a framework for activities which fall into the category of unacceptable use:

- Unauthorised copying of copyrighted material.
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojans, malware).
- Using a CTW computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment workplace laws.
- Sending unsolicited email messages including junk mail or other advertising material.
- Any form of harassment via email, whether through language, frequency or size of messages.
- Employees may not attribute personal statement, opinions or beliefs to CTW when engaged in blogging.
- Use of CTW's IT resources for other than CTW business which impedes CTW business or incurs a cost to CTW.

Approved Software

No software shall be installed or purchased unless it has been approved by the General Manager for use of CTW computers. Software will only be approved if CTW has a current licence to install and use the software if:

- it is fit for the intended use;
- the procurement procedure has been followed; and
- it will not endanger network security and the software can be supported either internally and have support/contract arrangements with external vendors.

Cyber Security

CTW ensures the continued operation of its cyber security planning and governance by:

- allocating roles and responsibilities to those accountable for cyber security including risks, plans and meeting the requirements of this policy,
- having an approved cyber security plan to manage CTW's cyber security risks, integrated with business continuity arrangements, which includes consideration of threats, risks and vulnerabilities that impact the protection of information, assets and services,
- remaining accountable for cyber risks of its ICT service providers and ensure the providers comply with the applicable parts of this policy. This includes providers notifying CTW quickly of any suspected or actual security incidents.

CTW builds and supports a cyber security culture by:

- implementing regular cyber security education for all employees, contractors and outsourced ICT service providers,
- increasing awareness of cyber security risks across all staff including the need to report security risks,
- fostering a culture where security risk management is an important and valued aspect of decision-making and where security risk management processes are understood and applied,
- ensuring that access is removed for people, who had access to sensitive information or systems, when they no longer need to know that information or their employment is terminated,
- sharing information on security threats across NSW Government to enable management of government-wide cyber risk.

CTW acknowledges it must improve its resilience including the ability to rapidly detect cyber incidents and respond appropriately.

Email Privacy and Content

Email should not be considered a private or secured form of communication as it may be forwarded or read by a third party. Content of emails should be carefully considered before sending.

Accessing Information Held in Protected Directories and Mailboxes

In a situation where a staff member is unavailable and information is required from their mailbox or directories for which they have exclusive access, this information can be retrieved by an IT Officer where:

- the need for the information is urgent and cannot wait for the availability of the authorised user; and
- a manager to whom the authorised user is responsible requests the information by email.

In a situation where the staff member is on extended leave and their email account needs monitoring, the IT Officer can provide access to their inbox to a designated CTW staff member following a written request via email from the relevant manager.

New Staff

A Fourier Technologies User Request Form is required to be completed and approved prior to creating network access.

Document No:	FT-FRM-SVC-004
Document Type:	Form
Form Name:	User Request Form
Approved By:	Management Team
Date Effective:	29/05/2019

User Request Form

Please complete this form for new users, existing users requiring additional access or to disable a user. Three (3) days' notice is required for new user accounts to be set up. Please send the completed form to support@fourier.com.au

Company Name:	
Location:	
Site Address:	

New User Access

This information will be used to create a new user logon in Active Directory, Microsoft Office 365 and a local computer login. If the new user requires a new computer, please log a separate ticket, where your Account Manager can provide a quote for your purchase approval.

New User First & Last Name:				
Position:				
Direct Phone No:		Mobile:		
Date New user commencing:				
Username to be created:		Default OU if known:		
Email address to be created:				
Additional email aliases or addresses:				
Does the New User require an O365 Licence?	No	Yes	E1	E3
Does the New User require the same access as another staff member or is the user replacing a staff member? Existing staff member to model account on:	No	Yes		
Shared mailboxes permissions to be added: *Please indicate Full Access only or Send As permission*				
Email Distribution groups to be added to:				
Is Remote Desktop access required?	No	Yes		
Network drives required:				
Printers required:				
Applications required:				
Does the New User have a Computer to use? Name of computer:	No	Yes		