Hawkesbury River County Council

Corporate Policy

Cyber Security

July 2022

DRAFT

Contact

Hawkesbury River County Council is located at:

6 Walker St
SOUTH WINDSOR, NSW, Australia
Phone 02 4587 2030
Post PO Box 6021, South Windsor, NSW, Australia
Fax 02 4587 0233
Email council@hrcc.nsw.gov.au
Website www.hrcc.nsw.gov.au

Office Hours
Monday to Friday
9.00am to 4:30pm

CONTENTS

1. OVERVIEW

1.1 Purpose

This policy outlines cyber security standards recommended for Hawkesbury River County Council. This policy is designed to be understood by all council staff and supported through the leadership structure.

1.2 Introduction

Cyber security covers all measures used to protect technology systems – and information processed, stored or communicated on these systems – from compromise of confidentiality, integrity and availability.

Hawkesbury River County Council has established effective cyber security policies and procedures and embedded cyber security into risk management practices and assurance processes. When cyber security risk management is done well, it reinforces organisational resilience, making entities aware of their risks and helps them make informed decisions in managing those risks. This policy will be complemented with meaningful training, communications, and support across all levels of the council.

1.4 Definitions

Council is Hawkesbury River County Council

Authorised User is a user who is authorised to access Council's IT facilities.

ICT Operations Manager is the officer in Council who has overarching responsibility for the provision, management and maintenance of Council's ICT Resources. At HRCC, that person is the General Manager.

Users include all Council employees, volunteers, work experience students, agency staff and contractors who use HRCC ICT resources and services.

Web Filtering is screening a Web page to determine whether some or all of it should be blocked to the user by checking the origin or content of a Web page against a set of rules pre-defined by Council.

Malware is Malicious software programs designed specifically to damage or disrupt a system, including viruses, worms etc.

Hardware can either be the external - physical parts of a computer and related devices, or internal - including motherboards, hard drives and RAM (Random access memory).

HRCC is Hawkesbury River County Council.

Application (App) refers to a computer software program.

Electronic Messaging includes all forms of digital written communication including and not limited to; email, instant messaging (Microsoft Teams), chat and SMS.

ICT Information, Communications and Technology.

ICT Resources is the technology used to store, process, access and manipulate information. HRCC ICT resources include but are not limited to all HRCC networks, including Local Area Networks (LANs), Wide Area Networks (WANs), and Portals; emails; hardware; software; servers; desktop computers; printers; scanners; portable devices; mobile phones and storage devices.

Personal Use is all use of Council ICT resources including internet usage, social networking and private emails that is not work related.

Mobile Data Service is a service offered by a mobile carrier that supports access to a computing network. A mobile data service allows mobile devices to connect to the internet.

Mobile Carrier is a company that provides the network services that allow voice and data transmission to and from a mobile device. For example, Optus is a mobile carrier.

Device is any piece of equipment that can be attached physically or wirelessly to a network or computer, for example, mobile phones, laptops, PCs, printers, keyboards, external disk drives, or other peripheral equipment.

Mobile Phone is a small hand-held mobile device that can utilise cellular based or Wi-Fi communication for the transmission and receipt of voice and data (through mobile phone apps).

Tablet can be a mobile device that provides computing facilities similar to a desktop or laptop computer but also uses Wi-Fi communications and/or cellular based communication for the transmission and receipt of messages, emails, and other data streams. Council uses tablet devices including the Microsoft Surface, Acer Spin the Apple iPad or Samsung devices.

Wi-Fi is a technology which allows devices to wirelessly connect to a data network and then access other facilities on, or through that network. Access to some Wi-Fi networks may require a password and/or payment. The most usual facility accessed through Wi-Fi networks is the Internet which also provides access to our business network and applications.

Professional or Business Use is any use of ICT resources that is for the business of Council.

Remote Work is an option for any staff to work from anywhere outside a Council Building(s) by using ICT resources such as – Laptop, Mobile Phone, Tablet or any other device.

The Internet of Things (IoT) describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

2. Policy

Council will implement cyber security **planning and governance**.

2.1 Roles and Responsibilities

Allocate roles and responsibilities as detailed in this policy.

The Council Roles listed in the below 'RACI' table are responsible for the following functions in support of this Policy. Responsibilities are referenced using the following legend:

	General Manager	Coordinator	Subject Matter Expert	All Staff
R Responsible — The person assigned to do the work **A** Accountable — The person who makes the final decision and has the ultimate ownership **C** Consulted — The person who must be consulted before a decision or action is taken **I** Informed — The person who must be informed that a decision or action has been taken				
Develop, Implement, Maintain and Support an Effective Cyber Security Policy	**A**	**R**	**-**	**I**
Implement Procedures, Practices, Training and Tools to assist with policy enactment	**R**	**R**	**C**	**I**
Design, Build, Implement and Maintain Cyber Security Procedures and Guidelines • Cyber Security Incident Response • Cyber Security Plan and Associated Reporting • Developing a metrics and assurance framework to measure the effectiveness of controls	**R**	**R**	**C**	**-**
Collaboration within HRCC • Ensuring that all staff and providers understand the cyber security requirements of their roles • Ensuring a secure-by-design approach for new initiatives and upgrades to existing systems, including legacy systems • Providing guidance on cyber security risks introduced from business and operational change • Incorporate Cyber Security into Risk Management Framework	**R**	**C**	**C**	**I**
Managing the life cycle of cyber security platforms including design, deployment, ongoing operation, and decommissioning	**R**	**A**	**C**	**I**
Validating that the cyber security plan meets the council's business goals and objectives	**A**	**R**	**-**	**I**

2.2 Executive Governance

Ensure there is a governance committee at the executive level (dedicated or shared) to be accountable for cyber security including risks, plans and meeting the requirements of this policy. Council needs to consider governance of ICT systems and Operational Technologies to ensure no gaps in cyber security related to items such as video surveillance, alarms, life safety and building management systems that use automated or remotely controlled or monitored assets including industrial Internet of Things (IoT) devices.

2.3 Business Continuity and the Cyber Security Plan

Develop, implement and maintain an approved cyber security plan that is integrated with HRCC's business continuity arrangements. This will include consideration of cyber security threats, risks and vulnerabilities that impact the protection of the Council's information, ICT assets and services.

2.4 Risk Management

Include cyber security in the risk management framework and consider cyber security threats when performing risk assessments.

2.5 Vendor Responsibilities

Be accountable for the cyber risks of ICT service providers and ensure the providers understand and comply with the cyber security requirements of the contract including the applicable parts of this policy (Section 4.1) and any other relevant Council security policies. This will include providers notifying the Council quickly of any suspected or actual security incidents and following reasonable direction from the Council arising from incident investigations.

3. Cyber Security Culture

Council will build and support a **cyber security culture** across their organization and related government bodies. Council will:

3.1 User Training

Implement regular cyber security awareness training for all Users.

3.2 Risk Aware Culture

Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied. This would involve increased awareness of cyber security risk across all users including the need to report cyber security risks.

3.3 Privileged User Access

Ensure that people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when they no longer need to have access, or their employment is terminated.

3.4 Security Threat Management

Share information on security threats and intelligence with Cyber Security NSW and cooperate across NSW Government to enable management of state-wide cyber risk.

4. Manage Cyber Security Risks

Council will **manage cyber security risks** to safeguard and secure its information and systems. Council will:

4.1 Information Security Management System

Implement a Cyber Security Framework with its scope at least covering systems identified as Council's "crown jewels".

4.2 Essential 8

Determine the levels of Maturity of the Australian Cyber Security Centre's (ACSC) Essential 8[1] Strategy that Council aims to achieve having regard to Council's cyber security risk assessment and resources and design a plan to achieve those levels.

[1] Strategies to Mitigate Cyber Security Incidents: https://www.cyber.gov.au/publications/essential-eight-explained

4.3 Information Classification

Classify information and systems according to their business value (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the requirements of the *Information Classification Labelling and Handling Guidelines* and

- assign overall responsibility for information asset protection and ownership
- implement controls according to their classification and relevant laws and regulations
- identify the Council's "crown jewels"

4.4 Cyber Security by Design

Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects. Any upgrades to existing systems will incorporate appropriate controls to ensure the solution remains within the organisation's cyber risk tolerance.

4.5 Auditing Requirements

Ensure new ICT systems or enhancements (i.e data analytics) include processes for audit trails and activity logging to assess the accuracy and integrity of data including processes for internal fraud detection.

5. Resilience

Council will improve their resilience including their ability to rapidly detect cyber incidents and respond appropriately. Council will:

5.1 Cyber Incident Runbook

Have a current cyber incident response plan that integrates with the business continuity plan.

5.2 Testing Procedures

Test their cyber incident response plan at least every year and involve the Leadership Team responsible for the management of media and external communications.

5.3 Monitoring Tools

Deploy monitoring processes and tools to allow for adequate incident identification and response.

5.4 Reporting

Report cyber security incidents to the Legal and Governance Team who in turn reports them to the Audit, Risk and Improvement Committee (ARIC) and liaises with insurance.

5.5 Exercises
Participate in or observe cyber security exercises as required.

6. Report against the requirements
Council will report **against the requirements** outlined in this policy and other cyber security measures for the previous financial year. Council will:

6.1 Compliance Report
Report annually on the compliance of the requirements outlined in this policy.

6.2 Essential 8 Report
Report annually the maturity against the ACSC Essential 8.

6.3 Risk Report
Report annually to the governing body Council's identified cyber security risks.