

	Function: INFORMATION TECHNOLOGY AND COMMUNICATIONS	Adopted: 2 nd March 2022 Resolution No.: C48:0322
	Policy Number: TC005	Last Review: 21 st January 2026 Resolution No.: C12:0126
	Version Number: 2	Next Review: January 2027
INFORMATION TECHNOLOGY SYSTEMS SECURITY GOVERNANCE POLICY		

1. POLICY OBJECTIVES

Copper Coast Council (Council) is committed to safeguarding Council's Information Technology (IT) infrastructure, digital assets, networks and Information (IT Systems) against the increasing risks of Security and cybercrime. This policy has been developed to:

- Support a secure technology environment through an integrated and systematic risk management approach;
- Govern acceptable use;
- Support continuous service improvement;
- Support legislative compliance and best practice;
- Foster a cyber Security culture.

2. SCOPE

This policy applies to all Council business activities and:

- Elected Members;
- Council Committees;
- Workers;

and other appropriately authorised Workers who have access to Council's IT Systems (Users).

3. DEFINITIONS

Definitions are provided in Attachment 1.

4. POLICY STATEMENT

Council operates in an ever changing technological world. Cybercrime and scams pose a significant threat to Council's IT Systems and, therefore, IT Systems Security is a vital business function. This policy provides the operating and monitoring security framework necessary to protect Council's IT Systems and ensure we can continue to do business.

It is essential that all Users:

- Are aware of the Security threats and the necessary protection measures that must be taken;
- Comply with all relevant Council policies and legislation when carrying out their day-to-day activities.

Any failure to comply may result in disciplinary action, up to and including dismissal.

Electronic version on Council N:/ drive is the control version. Printed copies are considered uncontrolled. Before using a printed copy, verify that it is the current version.

lifestyle location of choice

4.1 Information Technology Systems Access and Use

All Council IT Systems must be accessed and used in an effective, safe, ethical and lawful manner. It is the responsibility of every User to know what is required and ensure compliance.

Access to IT Systems is granted based upon business need. Users are only permitted to access and use IT Systems that they have been given the appropriate permission to access. Any other access is considered unauthorised.

Users must not:

- Use IT Systems for any unlawful or unethical activity;
- Engage in any activity which:
 - Causes, or could be construed as:
 - a. causing any form of harassment, discrimination or victimisation
 - b. abusive, profane, obscene, sexually explicit, offensive, violent, derogatory, defamatory or promoting hatred;
 - Violates or infringes the rights of others
 - Could cause IT Systems to be compromised in any way;
- Disclose any Confidential Information and/or sensitive Information;
- Upload any sensitive, internal or Confidential Information into Artificial Intelligence (AI) platforms of any kind;
- Intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce/remove any malicious code and Malware designed to self-replicate, damage, or otherwise affect the performance of, or access to any IT Systems;
- Without prior permission from ICT Coordinator or ICT Support Officer:
 - Download Software, Applications, script, games, music, movies or anything with Executable Code
 - Connect personally owned computing devices, computer peripherals, USB devices, digital cameras, etc. to IT Systems
 - Circumvent internet Security by using USB modems, personal hotspots, USB mobile wireless devices and mobile broadband cards
 - Alter or add to any IT Systems;
- Open files or click on links and/or attachments if the source is unknown, suspicious or untrustworthy;
- Distribute or click on any links provided or generated by Generative AI (GenAI),
- Access personal webmail accounts from Council supplied devices;
- Use IT Systems for personal business purposes;
- Change IT Systems Security settings.

Information must be:

- Protected based on its sensitivity, value and criticality;
- Created, modified, saved, transmitted or archived utilising Council's IT Systems

Electronic version on Council N:/ drive is the control version. Printed copies are considered uncontrolled. Before using a printed copy, verify that it is the current version.

and remains Council's property at all times.

External service providers must be evaluated to ensure, as best as reasonably practicable, that they are trustworthy and appropriately experienced. Third parties requiring access to Council's IT Systems must be appropriately authorised and monitored.

4.2 Artificial Intelligence (AI)

Genuine critical thinking and human oversight is crucial to good governance, due diligence and professional integrity. AI is not a substitute for critical thinking. While it can offer tremendous business opportunities, AI also poses a significant threat to Council's IT Systems including:

- The potential for Security risks/vulnerabilities to be introduced;
- Sensitive data leaks;
- There is no control over any content once it is entered;
- Paywalls, permissions and the legal rights of others may have been bypassed in compiling data sets;
- There is no audit trail.

AI platforms are largely driven by profit, rather than social/ethical good, and are not required to be:

- Peer reviewed;
- Truthful;
- Held accountable for content.

GenAI and LLMs can also be prone to Biases, ethical concerns and/or inaccuracies.

Users are **only** permitted to access and use Microsoft Copilot, unless otherwise appropriately authorised, to safeguard, as best as possible, Council's IT Systems and prevent data leakage/breaches. Any other GenAI, Large Language Model (LLM), Embedded AI must not be accessed/used.

Any User who relies upon an AI system is responsible for their own work and must be able to show evidence of how they reached a decision.

4.3 Security Incidents

Users must promptly report:

- Suspected IT System Security problems;
- IT Security alerts, warnings or suspected vulnerabilities;

to Council's ICT Coordinator or ICT Support Officer.

4.4 Risk Management

Effective IT Systems Risk Management is critical in ensuring Council maximises its opportunities, whilst minimising the significant risks. The associated risks are identified, analysed, evaluated, treated, managed, monitored and reported in accordance with Councils Risk Management Framework Policy GOV029, available via Council's www.coppercoast.sa.gov.au (Website).

5. RESPONSIBILITIES

Roles and responsibilities are provided in Attachment 2.

6. COMPLAINTS

Complaints relating to this policy must be in writing and lodged in accordance with Council's Complaints Policy GOV012, available via Council's [Website](#).

7. DELEGATION

Any applicable delegations are set out in Council's Delegations Register, available via Council's [Website](#).

8. REVIEW

This policy will be reviewed annually, to keep pace with the ever-changing cyber Security landscape, or more frequently as deemed necessary in consideration of any changes to legislation, relevant standards, codes and guidelines, audit findings and/or corrective actions/controls.

9. TRAINING

Council will provide User training and/or instruction as deemed appropriate.

Training needs will be reviewed during induction, individual performance reviews and as necessary in consideration of any changes to Council's IT Systems, legislation, relevant standards, codes and guidelines, audit findings, any corrective and preventative actions/Controls arising from Risk Assessment and/or hazard/incident reports and stakeholder feedback.

10. RECORDS MANAGEMENT

Records will be managed in accordance with Council's Records Management Policy RM001, available via Council's [Website](#).

11. POLICY AVAILABILITY

Policies are made available on Council's [Website](#) and can be:

- Inspected at Council's Principal Office, during ordinary office hours, without charge;
- Made available in electronic form without charge;
- Provided in printed format upon request and payment of a fee (if any), as set out in Council's Register of Fees and Charges (available via Council's [Website](#)).

12. REFERENCES AND LEGISLATION

Copyright Act 1968 (Commonwealth)
Electronic Communications Act 2000
Freedom of Information Act 1991
Independent Commissioner Against Corruption Act 2012
Local Government Act 1999
Ombudsman Act 1972
Public Interests Disclosure Act 2018
Spam Act 2003
State Records Act 1997
Surveillance Devices Act 2016
ISO27001 - IT Security Management Systems

ISO/IEC27002 - Information Security, cyberSecurity and privacy protection — Information Security controls

[Australian Public Service Commission](#) guidance documents including:

- [Policy for the Responsible use of AI in government](#)
- [Transparent Use of AI at the Commission](#)
- [Australia's AI Ethics Principles](#)
- [Shaping a future-ready HR with AI](#)

[Automated Decision-Making - Better Practice Guide](#)

[Information Privacy Principles Instruction \(IPPI\)](#)

[NSW Artificial Intelligence Assessment Framework](#)

[SA Government Guideline for the Use of Generative Artificial Intelligence and Large Language Model Tools](#)

13. RELATED COUNCIL OBJECTIVES, POLICIES AND DOCUMENTS

Strategic Plan 2025 – 2035

- Good Governance
 - Policies and Procedures
 - Risk Management
 - Continuous Improvement
 - Transparency and Accountability
- Leadership Commitments - Manage our finances and resources for a sustainable future
 - Operate with honesty and integrity and be accountable for the decisions we make

Records Management Policy RM001

Risk Management Framework Policy GOV029

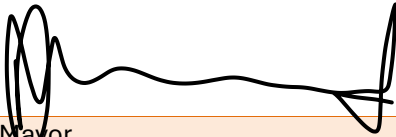
Code of Conduct for Employees 2020 HR021

Complaints Policy GOV012

Conduct Counselling and Discipline Policy HR014

Fraud Corruption Misconduct and Maladministration Prevention Policy GOV004

Behavioural Management Policy GOV028

Signed		
	Mayor	Chief Executive Officer
Date	20/02/2026	

Attachment 1 – Definitions

Applications	Software that performs specific tasks for an end-user.
Artificial Intelligence (AI)	Computer systems that are designed to simulate aspects of human intelligence. Most are underpinned by machine learning, which is an algorithm-based system that uses data patterns to learn and perform descriptive, predictive, and prescriptive tasks. Applications that include AI functionality include: • Virtual Assistants Including Apple's Siri, Amazon's Alexa, Google's Assistant and Microsoft's Cortana utilise AI to understand and respond to voice commands, perform tasks such as setting reminders, playing music, providing weather updates, and answering questions. • Recommendation Systems: Online platforms such as streaming services (Netflix, Spotify), e-commerce websites (Amazon), and social media platforms (Facebook, Instagram, Tik Tok), employ AI-based recommendation systems. These systems analyse user preferences, behaviours, and historical data to suggest personalised content, products, or connections. • Chatbots: AI-powered chatbots are used by businesses to provide automated customer support, answer frequently asked questions, and assist with basic enquiries. These AIs utilise natural language processing and machine learning techniques to understand and respond to user queries.
Bias	An inclination or prejudice for or against one person or a group of people that is unfair.
Confidential Information	Information: • Over which there is an order of Council or Council committee in effect under section 90 or 91(7) of the Local government Act 1999, requiring the Information or document to be treated confidentially; • That the Worker or former Worker knows, or ought reasonably to know, is Information that is otherwise required to be treated confidentially.
Deep Learning	A subfield of machine learning that employs artificial neural networks with multiple layers to learn and extract complex patterns and representations from data.
Embedded Artificial Intelligence	Artificial Intelligence technology that has been integrated into another device or system.
Executable Code	Machine language, which is the set of native instructions a computer carries out.
Generative Artificial Intelligence (GenAI)	A class of AI techniques that generate new content based on patterns and examples from existing data. It encompasses various algorithms and models designed to generate realistic and meaningful outputs such as images, text, music, or even entire virtual environments and can be used in various domains including art, entertainment, design, content creation, data augmentation and more. Underpinned by Deep Learning.
Hardware	A piece of computer equipment that makes up part of the physical computing environment.

Information	Data and/or records (as defined in Council's Records Management Policy RM001, available via Council's Website) in any format created or received through the conduct of Council business.
Information Technology (IT)	Hardware, Software and communications equipment, including, but not limited to: • Computers (including mobile computers) • Email • Internet • Mainframes • Wide and local area networks • Servers • Peripheral equipment • Telephones • Wireless communications • Public safety radio services • Facsimile machines • Technology facilities • Other relevant Hardware and Software items • Workers tasked with the planning, implementation, and support of IT.
Information Technology Systems (IT Systems)	Council's Information Technology (IT) infrastructure, digital assets, networks, internet access and Information.
Large Language Model (LLM)	A type of AI that once trained can recognise and interpret language and other types of data, that can generate textual content and retrieve existing content from their data set based on user input. Learning is based upon the patterns present in their training data.
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
Security	For the purpose of this policy, keeping IT Systems safe by: • Preventing unauthorised access, loss, corruption and interference • Protecting confidential and sensitive Information from disclosure.
Software	The programs and other operating Information that directly operates computer Hardware.
User	Elected Members, Council Committees, Workers and other appropriately authorised Workers who have access to Council's IT Systems.
Worker	All personnel undertaking tasks/duties for and/or on behalf of the Council, including persons employed directly by the Council in a full time, part-time or casual basis, volunteers, contractors, agency personnel, consultants and work experience/student placements.

Attachment 2 – Responsibilities

Roles	Responsibilities
Elected Members	Ultimate oversight and funding control over IT Systems. Defining Council's risk appetite. Ensuring the necessary: - Financial and other resources are invested in to protecting IT Systems; - Cyber Security structures and supports are in place to reduce the impact of cyber Security risks to Council.
Audit and Risk Committee (ARC)	Independent oversight of the Council's risk management practices, which incorporates IT Systems risks, including: - Reviewing risk management policies; - Monitoring risk mitigation efforts; - Reviewing cyber Security activities for effectiveness; - Providing independent assurance and advice to the Elected Body on risk management and governance matters.
Executive Management Team (EMT)	Administrative oversight and funding control over IT Systems. Responsible for ensuring that: - Appropriate Security structures and supports are in place to effectively manage IT Systems and reduce the likelihood and impact of Security risks; - Strategic IT Systems planning continues to meet the needs of the business; - The necessary financial and physical resources are invested in protecting IT Systems; - Initiatives to improve Information Security are approved and authorised as necessary; - Policies, procedures and supporting documentation are developed, implemented, published, communicated, reviewed and continue to meet business needs; - Adequate training is undertaken to ensure sound Security practices/controls are understood and effectively implemented by all Users; - Users have the equipment and skills to compliantly use Council's IT Systems; - Security risks are being appropriately managed; - Any significant change in Security threats exposure is identified and managed; - All Security incidents are monitored and reviewed; - Appropriate business continuity plans and incident response mechanisms are in place; - IT Systems Security controls across the organisation are co-ordinated; - Responsibilities for protecting IT Systems are clearly defined and allocated; - The necessary IT Systems are in place to protect and maintain Confidential Information;

Electronic version on Council N:/ drive is the control version. Printed copies are considered uncontrolled. Before using a printed copy, verify that it is the current version.

lifestyle location of choice

	• The purpose, use and implementation of any new IT Systems mechanism, channel or facility is appropriately approved as necessary; • There is transparency and accountability in decision-making processes; • Appropriate third party agreements, that contain at least the minimum Local Government Association Mutual Liability Scheme and Asset Mutual Fund standards, relating to Security and contractual requirements, are in place; • Specialist advice is appropriately funded and sought as and when required; • Users are aware of their IT Systems Security obligations; • Measuring and monitoring Security activities for effectiveness via Security activities reports, audit reports etc.
Managers	Oversee the IT Systems processes within their respective departments, including assisting in identifying, assessing and mitigating the risks associated with IT Systems. Provide guidance about the criticality and sensitivity of departmental processes to enable targeted Security risk management activities.
ICT Coordinator	Manage the Security risks associated with IT Systems by: • Identifying, assessing and mitigating the risks associated with IT Systems • Conducting vulnerability assessments; • Managing IT Systems projects; • Facilitating adequate training to ensure sound Security practices are understood by all Users and; • Monitoring and measuring cyber Security activities for effectiveness and regular, scheduled reporting to the EMT and ARC; • Developing, implementing, communicating and reviewing policies, procedures and supporting documentation that continue to meet business needs; • Ensuring: ○ Appropriate IT Systems/processes are in place to protect and maintain Confidential Information; ○ Compliance to the appropriate/relevant legislative requirements, standards and best practice protocols; ○ Effective Security controls are implemented; ○ IT Security Systems are Implemented, deployed and utilised ○ Appropriate business continuity plans and incident response mechanisms are in place; ○ Any significant change in Security threats exposure is identified and managed; ○ All Security incidents are monitored and reviewed; ○ IT Systems Security controls across the organisation are coordinated.

Corporate Governance Officer	Assist in identifying, assessing, mitigating and auditing the risks associated with IT Systems.
Governance Officer	Assist with measuring and monitoring of IT System activities for effectiveness.
Coordinator WHS and Risk	Assist in developing and implementing appropriate business continuity plans.
Users/Workers	Ensure that their use of IT Systems is consistent with their duties and obligations under the Local Government Act 1999 and any other relevant legislation. Must read, understand and comply with Council's IT Systems Policies, Procedures and supporting documentation.