1.23 Cyber Security and Information Systems Security

POLICY TITLE: CYBER SECURITY INFORMATION SYSTEMS SECURITY

FILE REF: SC490

EXPIRY DATE: OCTOBER 2027

OBJECTIVE

Information is an important, valuable asset of Council which must be managed and protected. All information has a value to the Council. However, not all information has an equal value or requires the same level of protection.

The aim of this Policy is to protect information against accidental or malicious disclosure, modification or destruction.

The Policy also establishes policy principles and parameters for the development of procedures to help identify, prevent, mitigate and recover from malicious attacks on Council's electronic information systems that may lead to data theft, unauthorised changes to information systems, fraud, business interruption, reputational damage and other related security risks.

SCOPE

This Policy applies to all Councillors, Staff, and Volunteers of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Council with any form of access to Council's electronic information systems.

REFERENCE DOCUMENTS

This Policy should be read in conjunction with the following Council policies and documents:

a) Policy 1.7 Fraud Control Policy

b) Policy 3.26 Computer, Internet, Email and Social Media Policy

c) Cyber Security Procedures

INTEGRATED PLANNING AND REPORTING REFERENCE

This Policy, and the Cyber Security Procedures developed in accordance with the Policy, align with the objectives, strategies and actions contained in the Council's 2022-2032 Community Strategic Plan and 2026-2028 Delivery Plan as follows:

a) Minimise Council's exposure to risk and promote a strong risk management culture within Council.

b) Ensure appropriate IT systems are in place to support service delivery and accountability requirements.

c) Maintain and develop a Records Management System that meets the needs of the organisation, the community and legislative requirements.

DEFINITIONS

Cyber security – the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. It's also known as information technology security or electronic information security.

Cyber-attack – an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A cyber-attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks.

Information security controls – measures taken to reduce information security risks such as information systems breaches, data theft, and unauthorized changes to digital information or systems.

IP Address – IP stands for Internet Protocol and an IP address is a unique address that identifies a device on the internet or a local network. In essence, IP addresses are the identifier that allows information to be sent between devices on a network. They contain location information and make devices accessible for communication.

The Essential Eight –a series of baseline mitigation strategies taken from the Strategies to Mitigate Cyber Security Incidents recommended for organisations by the Australian Cyber Security Centre (ACSC).

Vulnerability scanning – an assessment that's performed without access to the network that's being scanned. External scans target external IP addresses in one's network, identify vulnerabilities as well as all the ports that can be accessed from the internet.

Multi-factor authentication – when a user must provide two or more pieces of evidence to verify their identity to gain access to an application or digital resource. Multi-factor authentication is used to protect against hackers by ensuring that digital users are who they say they are.

SECURITY VETTING

Any person wanting to access the Lockhart Shire Council's information systems must be authorised to do so.

Potential new users of the Council's information systems and assets must be identified, vetted and authorised before being given access to resources appropriate to their role.

Levels and areas of access approved are based on the following classifications:

a) **Employees** – Employees are employed under the Local Government (NSW) State Award and are required to comply with Council policies and codes. Employees are vetted and given access to information systems appropriate to their role and delegations as part of their induction process. Employees are also trained in the particulars of Council's information technology (IT) systems relevant to their role. Council's Handbook for New Employees draws attention to relevant codes and policies including the Code of Conduct and Policy 3.26 Computer, Internet, Email and Social Media.

b) **Councillors** – Councillors are elected by the Shire's residents and ratepayers in accordance with the Local Government Act and are required to comply with Council policies and codes relevant to their role or as legislated e.g., Code of Conduct. Councillors are provided with access to Council meeting business papers, including confidential reports, through a secure portal via Council's website.

c) **Privileged Users** – Privileged users are those given special access rights to the network to carry out specific maintenance functions and include the Council's software suppliers, IT contractors and specialists. Their work is to be always carried out under the supervision of the Director of Corporate and Community Services.

CYBER SECURITY PROCEDURES

Cyber Security Procedures will be developed and maintained that, as far as practicable, have regard to the Essential Eight baseline strategies recommended by the ACSC as follows:

Prevention (prevent attacks)

1. Software Protection

   Anti-virus software incorporating firewalls and other mechanisms that guard against cyber-attacks are to be installed and maintained on Council's information systems.

2. Application Control

   Only approved applications are to be executed on Council's IT systems. Under no circumstances are software products not owned by or not legally in possession of the Council to be installed on Council equipment. Software obtained in confidence or under licence must only be used by staff members or authorised agents of the Council in accordance with relevant licence agreements.

   Proposals for purchase of software for official Council purposes are to be directed to the Director of Corporate and Community Services.

3. Patch Applications and System Change Management

   An important component of cyber security is ensuring that software applications and operating systems remain up to date. Updates are commonly referred to as "patches" and are released by the third-party vendor from whom the application has been purchased.

   This is particularly important for Council's financial and accounting software, Practical Plus, provided by Civica. The Procedures are to ensure that all changes made to Practical Plus are subject to appropriate testing and approval prior to implementation to prevent unauthorised or untested changes that may adversely impact Council's operations.

4. Email Attachments and Internet Documents

   Files opened from an internet location or received as a Microsoft Outlook attachment can have viruses and other harmful content embedded in them.

   As a security measure the "automatically download attachments" setting is to be "turned off" and attachments from external emails and documents sourced from the internet are in the first instance to be opened in "Protected View".

5. Vulnerability Scanning

An external vulnerability scan is an assessment that's performed without access to the network that's being scanned. External scans target external IP addresses in one's network, identify vulnerabilities as well as all the ports that can be accessed from the internet.

Periodic vulnerability scanning is to be performed on Council's externally facing IP Addresses in consultation with Cyber Security NSW.

6. Reports and Alerts

Cyber security is a dynamic and rapidly changing field. In order to remain abreast of developments Council will engage with Cyber Security NSW which provides information, guidance and assistance with cyber security matters including alerts issued in relation to critical vulnerabilities and software releases as well as intelligence briefs in relation to ransomware operators, targeted victims and other emerging trends.

7. Training and Education

Employees can be the first and last line of defence against cyber threats and for this reason having a cyber security training program is vital.

Cyber Security Awareness training is to be provided to all staff with access to Council's electronic information systems and form part of the induction program for new employees.

Mitigation (limit extent of attacks)

1. Restrict administrator and user privileges

Users of Council's electronic information systems will be given privileges and access rights that are commensurate with the tasks they are expected to perform.

When an employee leaves the Council their access to information systems and data is to be suspended at the close of business on the employee's last working day.

A periodic review of access rights will be undertaken to ensure all existing users are authorised to retain access and that the level of access provided to each user is commensurate with the tasks they are expected to perform.

2. Multi-factor authentication

All users must be allocated access rights and permissions to electronic information systems and data that require multi-factor authentication to protect against hackers by ensuring that digital users are who they say they are.

Recovery (recover data and system availability)

1. Back-ups

In order to regain access to electronic data in the event of the loss or unavailability of data processing systems, data back-up procedures will be established and maintained to ensure a daily back-up copy of Council's data is maintained "off-site".

2. Security Incidents

Security incidents are events in which the security of the Council's intellectual property or information assets is actually or potentially compromised.

The Cyber Security Procedures will provide for the investigation of security incidents to determine exactly what occurred, assess the degree of compromise of information, operations or resources, and make recommendations to minimise the possibility of the incident re-occurring.

Significant breaches are be reported to Cyber Security NSW via report@cyber.nsw.gov.au.

If the breach is of a serious nature involving criminal activity, or compromise of very sensitive information, the incident is to be reported to the Police.

RECORD KEEPING

All records pertaining to system change management and periodic reviews of user access are to be registered in Council's electronic document and records management system, Content Manager 9.

Details of cyber awareness training provided to employees with access to Council's electronic information systems is to be maintained on individual employee files.

A Register is to be maintained containing the dates and times that periodic vulnerability scanning is performed by Cyber Security NSW together with information regarding the results of the scanning and any action taken in response to those results.

A Register of security incidents is to maintained recording the details of each event and the action taken if any.

MONITORING OF INFORMATION SYSTEMS

On a continuous and ongoing basis Council may carry out computer surveillance of any user at such times of Council's choosing and without further notice to any user in accordance with Policy 3.26 Computer, Internet, Email and Social Media.

Adopted by Council, 21 October 2024
Refer Minute No. 159/24

Adopted by Council 18 October 2021
Refer minute 195/21