CYBER SECURITY FRAMEWORK

BROKEN HILL
CITY COUNCIL

AUSTRALIA'S FIRST
HERITAGE LISTED CITY

BROKEN HILL
CITY COUNCIL

QUALITY CONTROL

KEY DIRECTION	4. Our Leadership		
OBJECTIVE	4.2 Ensure Council has robust Information Communications Technology Platform		
FUNCTION	Leadership & Governance		
STRATEGY	4.2.3.1 Continue to implement the agreed Information and Communication Technology Strategy/Roadmap		
FILE REFERENCE No	18/142	**TRIM No**	D21/10467
RESPONSIBLE OFFICER	Manager Information Services		
REVIEW DATE	June 2023		

DATE	ACTION	MINUTE No
30 June 2021	Public Exhibition	46564
25 August 2021	Adoption	46618

TABLE OF CONTENTS

1. INTRODUCTION

Broken Hill City Council (Council) depends up on reliable critical technology infrastructure to deliver services to the community and to facilitate business and governance functions. Cyber security threats exploit the complexity and connectivity of critical infrastructure systems, placing the organization and the public at risk. These threats can result in financial and reputational risks, create legal challenges and result in non-compliance of the law.

At council, the Cyber Security Framework is underpinned by the Information Services Standards Library which outline the rules and guidelines around system management, operation and use.

2. FRAMEWORK OBJECTIVE

The Cyber Security Framework has been developed to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of Council.

For the purposes of this document "Cyber Security" refers to the measures relating to the defence of Council systems from attack and "Information Security" refers to measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.

The Cyber Security Framework is a risk-based framework developed to assist with preserving the confidentiality, integrity and availability of information by applying risk management processes, with increasing control measures to be implemented based on increased likelihood or impact. A risk-based approach to cyber security management provides flexibility to implement controls based on risk profile, as opposed to a one-size-fits-all approach.

The framework outlines the mandatory requirements to which all staff must adhere as well as a set of supporting expectations. This document is designed to be used by all personnel within Council including senior leadership, managers, information services staff, audit and risk teams.

3. FRAMEWORK SCOPE

Relevant sections of the Cyber Security Framework will also apply to contractors working for/with Council as well as suppliers that provide goods to Council.

4. FRAMEWORK STATEMENT

The Cyber Security Framework is supported by a significant suite of supporting documentation, guidance and templates from the Information Services Standards library to help employees implement the framework based on their risk profile and in line with an existing IT policies and procedures.

4.1 Council Policies

- Email, Internet and Computer Systems Usage Policy.
- Mobile Telephone Policy.

4.2 Operational Policies

- Information Services Standards Library.

4.3 International Standards

- ISO27001 – Information Security Management System.
- ISO27002 – Code of practice for information security controls.

4.4 Australian Strategies

- Australian Cyber Security Centre Essential 8 Security Mitigation Strategies.

5. IMPLEMENTATION

5.1 Roles and Responsibilities

The following Council Officers are responsible for the implementation of and the adherence to this framework:

- General Manager
- Chief Financial Officer
- Manager Information Services
- Information Services Staff
- Council Staff, Contractors, Suppliers and Volunteers

5.2 Communication

This framework will be communicated to all staff and available electronically.

All Council employees will have access to Operational policies via Council's Intranet and Council policies via Council's website. The community will have access to Council policies via Council's website. Access to procedures and processes will be available via Council's electronic information management system (Content Manager).

5.3 Associated Documents

- D12/1833 – Email, Internet and Computer Systems Usage Policy
- Information Services Standards Library available at https://ITStandards.brokenhill.nsw.gov.au
- D21/9990 – Australian Cyber Security Centre - Essential Eight Explained (June 2020)
- D21/9991 – Australian Cyber Security Centre - Essential Eight Maturity Model (June 2020)
- D21/9994 – Australian Government Information Security Manual (March 2021)

6. PRINCIPLES AND POLICIES

The Cyber Security Framework consists of 20 policy statements underpinning the principles of Governance, Information, Personnel and Physical.

Principle: Governance		
Manage security risks and support a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.		
Leadership	Staff Responsibilities	Risk Management
Policies, Procedures and Compliance	Audit (Internal and External)	
Principle: Information		
Maintain the confidentiality, integrity and availability of all information and systems to an appropriate level, depending on the information classification.		
Information Asset Identification and Classification	Incident Management	Resilience and Service Continuity
Access to Information	Administrative Access	Vulnerability Management
System and Software Acquisition	Cloud Computing	Network Communications
Mobile Device Management	Teleworking	Robust ICT Systems and Operations
Principle: Personnel		
Ensure employees and contractors are suitable to access Council resources and meet an appropriate standard of integrity and honesty.		
Awareness	Personnel Security Lifecycle	
Principle: Physical		
Provide a safe and secure physical environment for people, information and assets.		
Physical Security		

6.1 Policy and Expectation Statements

POLICY STATEMENT	EXPECTATIONS
6.1.1 - Leadership Senior leadership is ultimately accountable for the implementation and effectiveness of the council's cyber security program. Senior leadership must be actively engaged in cyber security initiatives and champion cultural change.	• Cyber security is regularly included in the agenda of an appropriate senior leadership body, ensuring discussion is focused on the progress of the cyber security program and cyber security risks to the council, both existing and emerging. • Senior leadership allocates roles, responsibilities and resources to support and enable the Council's Cyber Security Program.
6.1.2 - Staff Responsibilities Roles and responsibilities for cyber security must be formally assigned by senior leadership, demonstrating commitment to providing suitable resources to manage the council's cyber security program. Personnel and contractors must be provided with information and training to support awareness of their collective responsibility to foster a positive security culture.	• Council has appointed a leader accountable for cyber security to provide strategic level guidance for the council's cyber security program and ensure compliance with cyber security policy, standards, regulations and legislation. • Responsibility for day-to-day cyber security operations is assigned and documented in policy and relevant position descriptions. • Cyber security education and awareness training is provided to all personnel and contractors during induction and at least annually thereafter, ensuring they are aware of their responsibilities regarding the appropriate use of council information assets. • Skills gap assessments are performed for cyber security and IT personnel responsible for implementing or managing technical security controls. Targeted training is provided for these personnel specific to the technologies in use within the organisation. Where contractors or third parties are used in place of internal resources, contract staff are held to the same standards as staff.
6.1.3 - Risk Management The council must take steps to identify, understand, assess and manage cyber security risks to its critical processes and information assets. Cyber security risk management processes must be embedded within the council's risk management framework and align to the risk appetite of the council. Senior leadership must be aware of current and emerging cyber security risks to the organisation.	• Cyber security risks are documented in a cyber security risk management matrix maintained by IT and Risk personnel and periodically reviewed by the Audit Committee.

6.1.5 - Audit (Internal and External) Cyber security is regularly assessed by both internal and external audits. A program of cyber security assurance activities must be in place to evaluate the effectiveness of the council's cyber security program and ensure cyber security controls are implemented and operated in accordance with the council's policies and procedures, relevant laws, regulations and contractual requirements and this framework.	• Independent reviews are performed periodically in line with council requirements. • Technical security reviews of critical systems are planned and carried out using a risk-based approach.

6.2 Principle: Information

POLICY STATEMENT	EXPECTATIONS
6.2.1 - Information Asset Identification and Classification Information assets supporting critical processes must be identified, recorded and classified. Processes must be in place for labelling, storing, handling and disposing of information assets in alignment with their classification.	• Information assets supporting critical processes are identified and recorded in an information asset register. • Information assets are formally assigned an owner.
6.2.2 - Incident Management Cyber security incident response plans must be in place and aligned with an overarching incident management process to enable a consistent approach to the management of cyber security incidents.	• Cyber security incident response is included in the Council's BCP, documenting responsibility for cyber security incident management. • Testing of incident response plans is included in assurance activities. • Post-incident reviews are performed and evidence relevant to cyber security incidents is recorded and retained. • Reporting of breaches that fall under the federal Notifiable Data Breaches (NDB) legislation occurs.
6.2.4 - Access to Information Access to council systems, applications and information must be based on business need, authorised by the information owner or delegated custodian and be limited to the minimum required for personnel to undertake their duties. Secure authentication mechanisms must be in place to control access to council systems, applications and information.	**Access Provisioning:** • Physical or logical access to council information assets is provided based on business need and least-privilege principles. • The processes to provision access to systems and applications in use within the council are documented. • Authentication and Traceability. • All users have unique accounts providing traceability of actions within critical systems and applications.

	• Secure encrypted remote access technologies are used to remotely access the council's IT environment. • User password standards (complexity, minimum length, maximum age) are documented and implemented on all systems and applications. • Multi-factor authentication is required to authenticate users to systems supporting this technology when not accessed from regular workstations and/or locations. • Certificate based authentication is implemented to identify authorised workstations connected to the council's network. **Access Reviews:** • Reviews of user access are performed at least annually for the network and all critical applications. • Termination of Access. • Terminated user's access is revoked within defined timeframes.
6.2.5 - Administrative Access Administrative access to council systems, applications and information must be restricted to personnel with a specific business need which is validated on a periodic basis.	**Access Provisioning:** • IT users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access. • Technical controls are in place to restrict the use of privileged accounts from reading emails, accessing the internet and obtaining files via online services. • Everyday use accounts do-not have local administrative privileges on workstations and servers. **Access Reviews:** • Reviews of privileged user access are performed at least every six months. **Authentication and Traceability:** • Privileged account actions deemed high risk by the council are logged and monitored for unusual activity. • Password standards (complexity, minimum length, maximum age) for privileged accounts are documented and implemented on all systems and applications. • Multi-factor authentication is required to authenticate privileged users in all systems supporting the functionality. **Termination of Access:** • Privileged access is revoked immediately once there is no longer a specific business need for it.

6.2.6 - Vulnerability Management Security vulnerabilities in council ICT equipment, systems and applications must be identified and managed.	• Security vulnerabilities in applications and operating systems are patched or mitigated within one month of fix release for all workstations and servers. • Security vulnerabilities in applications and operating systems that are assessed as 'extreme' are patched or mitigated within 48 hours of release for all workstations and servers. • There is a documented process for managing the risks associated with non-vendor supported applications and operating systems where they are required for a specific purpose. • A mechanism is in place to ensure compliance to patching requirements. • Malware detection and prevention tools are in place on all workstations and servers. • A vulnerability management process is in place that includes: o Conducting vulnerability assessments and network penetration tests for key systems throughout their lifecycle to identify security vulnerabilities. o Analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations or treatments based on effectiveness, cost and existing security controls. o Using a risk-based approach to prioritise the implementation of identified mitigations or treatments. o Monitoring information on new or updated security vulnerabilities in operating systems, software and ICT equipment as well as other elements which may adversely impact the security of a system.
6.2.7 - System and Software Acquisition Cyber security requirements must be considered throughout the acquisition lifecycle for acquiring new systems and software	• Security risks associated with system and software acquisition or significant system enhancements are identified, documented and managed as per the council's risk management framework before the system and/or software is implemented into production. • Where system acquisition relates to a cloud service, the requirements of 2.8 Cloud Computing are applied.
6.2.8 - Cloud Computing Risk assessments must be performed by the council prior to implementing any cloud computing service in order to assess the benefits of the service balanced with the additional jurisdictional, governance,	• A risk assessment is performed before implementing any cloud service. • Security risks associated with a cloud service are identified, documented and managed as per the council's risk management framework before the cloud service is implemented.

privacy and security risks associated with the use of such services	• Cloud services fully hosted within Australia, subject to Australian laws are preferred.
6.2.9 - Network Communications Network communications must be secured, ensuring council information traversing internal and external networks can only be accessed by authorised parties.	• The council's network architecture is documented showing the internal network structure and incoming/outgoing egress points. • Information flows associated with critical processes are documented listing: o The type of information, o The classification of the information, o Who the information is being exchanged with? o The controls in place to protect the information. o Network segregation is implemented throughout the council's network.
6.2.10 - Mobile Device Management Technical and procedural controls must be in place to address the risks associated with the use of mobile devices including mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet connected devices.	• Procedural controls have been established, outlining the mechanisms for protecting council information stored on or accessed from laptops, mobile phones and removable storage devices. • Processes exist for requesting and authorising the use of personal mobile phones to access council information such as emails. • Passphrases and/or PIN codes are in place on laptops and mobile phones used for accessing council information. • Encryption of storage is enabled for all laptops, mobile phones, and removable storage devices • A mobile device management solution is in place to ensure that appropriate controls are applied to all mobile phones, including personal phones used for work. • Remote wipe functionality is enabled for all council laptops and mobile phones, including personal phones used for work.
6.2.11 - Teleworking Secure practices for teleworking must be established and understood by council personnel, with technical controls implemented to enable secure remote access to council information.	• Teleworking procedures are established and socialised with council personnel working offsite. • Technical controls are implemented to enable secure remote access to council information assets.
6.2.12 - Robust ICT Systems and Operations Standard operating procedures and technical controls must be in place to provide a consistent and secure approach	**Standard Operating Procedures:** • Standard operating procedures have been developed for all primary cyber security functions performed by council personnel.

to system administration, maintenance and configuration activities.	**Change management:** • A change management process is developed and implemented that includes: • Identification and documentation of changes to be made, • Approval required for changes to be made, • Implementation and testing of approved changes, and • Any actions to be taken before and after approved changes are made. **Backups:** • Backup, restoration and preservation strategies are developed and implemented as part of business continuity, disaster recovery and information preservation planning. • Backups of important information, software and configuration settings are performed at least daily and stored for at least three months. • Backup and restoration processes are tested annually. • Backups are stored offline, or online in a non-rewritable and non-erasable manner. • Full back up and restoration processes are tested when fundamental IT infrastructure changes occur. **System Configuration and Hardening:** • Macro settings within Microsoft Office are as follows: o Only signed Microsoft Office macros can execute. o Microsoft Office macros in documents originating from the Internet are blocked. o Microsoft Office macro security settings cannot be changed by users. o Web browsers are configured to block or disable support for Flash content, web advertisements and Java from the Internet. o Technical controls are in place to restrict non-privileged users from installing software. • Application whitelisting is implemented on all workstations and servers to restrict the execution of executables and software libraries to an approved set. **Event Logging and Monitoring:** • An event logging strategy is developed and implemented covering events to be logged, logging facilities to be used, event log retention periods and how event logs will be protected.

	• A centralised logging facility is implemented, and systems are configured to save event logs to the centralised logging facility as soon as possible after each event occurs. • An accurate time source is established and used consistently across systems and network devices to assist with the correlation of events.

6.3 Principle: Personnel

POLICY STATEMENT	EXPECTATIONS
6.3.1 - Personnel Security Lifecycle Current/Separating personnel must be made aware of their ongoing cyber security obligations.	• New/Current staff are offered cyber security awareness training and annually sign-off on their obligations. • Separating personnel are made aware of their ongoing cyber security obligations, and have their access to council resources withdrawn, per user access management processes.

6.4 Principle: Physical

POLICY STATEMENT	EXPECTATIONS
6.4.1 - Physical Protection Protective security must be integrated in the process of planning, selecting, designing and modifying council facilities for the protection of people, information and physical assets.	• Physical security measures are in place to protect council physical assets including people, information and facilities based on the classification of the information that they are approved for processing, storing or communicating.

7. REVIEW

The review of this framework shall be undertaken within two years and will incorporate consideration of relevant legislation and best practice guidelines. The responsible Council officer will be notified of the review requirements three months prior to the expiry of the Framework.

Council's Manager Information Services is responsible for the review of this Framework.

8. DEFINITIONS

In this Framework the following definitions will apply:

Classification – shall mean the process by which information assets are labelled according to their business importance and sensitivity. Classification ratings are used to indicate the value of the information.

Council – shall mean Broken Hill City Council.

Council Policies – shall mean policies regarding specific statutory, strategic or administrative direction and adopted, amended and reviewed by Council with a minute number recorded.

Critical Processes – shall mean Council processes that, if not performed, would eventuate in the highest level of risk to the organisation. This could include meeting critical needs of the organisation or satisfying mandatory regulations and requirements.

Critical Service – shall mean services that, if compromised, would result in significant damage to the physical, social or economic wellbeing of the LGA. Critical Services are not typically ICT services, they are services that an agency delivers to the community.

Cyber Security – shall mean measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.

Delegation – shall mean the delegated authority from the General Manager to Council officers.

Encryption – shall mean the process of converting information or data into a code, especially to prevent unauthorized access.

Extreme Vulnerability – Defined as:

- the security vulnerability facilitates remote code execution,
- critical business systems are affected,
- an exploit exists in the public domain and is being actively used, and/or
- the system is internet-connected with no mitigating controls in place.

Framework – shall mean a basic conceptual structure used to solve or address complex issues.

LGA – shall mean Local Government Area.

Governance – shall mean the exercising of authority or decision-making processes.

ICT – shall mean Information and Communication Technology.

Operational Policies – shall mean policies regarding operational and employment matters and approved by the General Manager.

Policy – shall mean a high-level statement that establishes the basis and framework for conduct and practice by and at Broken Hill City Council. It is the 'what' and 'why' of Council decision-making. Policies will typically be brief and rely on other means to give effect to their direction.

Policy, Procedure and Process Statements – shall mean the communication of the specific detail and course of action that will be adhered to by Council and its employees.

Policy Type – shall mean either "Council Policy" or "Operational Policy".

Procedure – shall mean a document written to support a "policy or organisational directive" and designed to describe who, what, when and why in order to establish corporate accountability.

Process – shall mean the documentation of the "how" to steps for the completion of a task or function.

Security Incident – shall mean a security incident is an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed. Loss/degradation of service, corruption of data or breach of privacy are likely outcomes.

Information Assets – shall mean any information or asset supporting the use of the information that has value to the organisation, such as collections of data, processes, ICT, people and physical documents.

Information Custodian – shall mean the individual or group assigned responsibility for managing a set of information.

Information Owner – shall mean the individual or group responsible and accountable for a set of information. The information owner may, at their discretion, assign responsibility for management of the information to another person or group, also known as an information custodian.

Mobile Device – shall mean mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices.

Multi-factor – shall mean a method of authentication using separate mutually dependent credentials, typically "something you have" and "something you know".

BROKEN HILL

CITY COUNCIL

www.brokenhill.nsw.gov.au