Cyber Security Policy

Responsible Officer: Group Manager Corporate & Commercial (Guy Bezrouchko)

Recommendation

That Council:

1. Revoke the Records Management policy dated 18 June 2014, and any policy revised as a result of that revocation; and
2. Adopt the draft Cyber Security policy attached to this report.

Background

The Audit Office of NSW issued a Final Management Letter for the Year Ended 30 June 2019 which noted that:

- Council does not have a specific cyber-security framework, including formal policies and procedures covering the identification, protection, detection, response and recovery of information systems.
- Lack of a formal cyber security framework / policy increases the risk that Council is less prepared to identify and respond to cyber incidents in the most effective way.

The attached proposed Cyber Security policy has been formulated to address these issues.

1. Proposed Cyber Security policy

The proposed Cyber Security policy has been developed to:

(a) provide a set of security controls to regulate the use, passage, and storage of cyber within Council in addition to applicable Legislative requirements

(b) help protect Council and to minimise the risk that might result from inappropriate use of Council cyber.

(c) establish a consistent policy position for cyber security

(d) have a current cyber incident response plan that integrates with the Council incident management process

(e) develop a cyber security strategy, architecture, and risk management process and incorporate these into the agency's current risk framework and processes.

2. Policy for revocation and ancillary procedures

The following table identifies the policy to be fully or partially consolidated into the proposed Cyber Security policy or incorporated into a procedure:

Policy	Justification for revocation
'Records Management' policy dated 18 June 2014	Fully incorporated into the proposed 'Cyber Security' policy and accompanying procedures. *

* A number of procedures will be developed and will be approved by the General Managerand Leadership Team post adoption of this policy

Governance

The proposed policy has been informed by Cyber Security NSW cyber security policies / frameworks. Those documents have been developed for state government agencies and the policy in particular notes: *"This policy is not mandatory for state owned corporations, however it is recommended foradoption in state owned corporations, as well as local councils and universities".*

Consultation

A consultation exercise was undertaken between subject matter experts within Council and external industry consultants in the development of the proposed Cyber Security policy.

Conclusion

Relevant content contained in the policy put forward for revocation has been captured within the proposed Cyber Security policy, procedures and/or standard operating procedures as appropriate.This has been done in consultation with relevant Records staff.

The proposed Cyber Security policy is submitted to Council for adoption.

Attachments

1. Cyber Security policy (for adoption)
2. Records Management policy dated 18 June 2014 (for revocation)

Attachment 1

Policy

ROUS COUNTY COUNCIL

Cyber Security

Approved by Council: xx/xx/xxxx

To set out the mandatory requirements for management of cyber security risks to information and systems.

Safety Teamwork Accountability Respect

Policy statement

To ensure Council's Information and Communication Technology ('ICT') systems are fit-for-the-future, Council has adopted a hybrid operating model known as a 'cloud first' strategy. This strategy will reduce the risks associated with on-premise systems and better promote achievement of Council's business objectives.

A robust and mature cyber security program is critical to the achievement of Council's business objectives. Council's cyber security program consists of a number of mandatory requirements and has been informed by and is modelled on the NSW Government Cyber Security Policy which is recommended as a foundation of strong practice for local councils.

This policy applies to all systems, people and processes that constitute the Council's information systems including, but not limited to, councillors, employees, ICT service providers, contractors, and all other parties with access to Council's ICT systems

Mandatory requirement 1

LEAD	*By implementing cyber security planning and governance.*

1.1 Adopt and maintain an Information Security Incident and Data Breach Response Plan that integrates with Council's Business Continuity Plan.

1.2 Develop and implement Security Procedures that support the objectives of this Policy; to be reviewed annually.

1.3 Develop and maintain an ICT Risk Register which will include cyber security risks.

1.4 Ensure cyber security minimum requirements are documented and built into procurement governance including requirements for bespoke ICT systems and assets.

1.5 Require third party ICT service providers, as a condition of engagement, to adhere to requirements for, among other things, the reporting and investigation of any suspected or actual security incident.

1.6 Consider cyber security threats when performing risk assessments and include 'high' and 'extreme' risks in Council's overall risk management framework.

Mandatory requirement 2

PREPARE	*By promoting organisation wide cyber security culture and accountability.*

2.1 Implement regular cyber security education for all employees and contractors, including roles and responsibilities outlined in this Policy, and expectations on reporting of cyber security risks.

2.2 Ensure that third party ICT service providers understand and implement Council's cyber security requirements as a condition of contract.

2.3 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.

2.4 Ensure approval and screening processes are appropriate and consistently used to govern and regulate access to Council systems and information using the principle 'minimum access required to do the job'. This includes the timely removal of access when no longer required or when employment is terminated.

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

Mandatory requirement 3

PREVENT	*By safeguarding information and systems.*

3.1 Ensure all devices, ICT systems and physical assets are secured in accordance with the Security Procedures.

3.2 Undertake the design, development, deployment, and maintenance of new ICT systems, or enhancements to existing ICT systems or decommissioning of ICT systems, in accordance with the Security Procedures and in consultation with the ICT Manager.

3.3 Ensure all new ICT systems, or enhancements to existing ICT systems, comply with national standards and any relevant international standards where appropriate.

3.4 Implement Security Incident Management Response Procedures.

3.5 Ensure ICT systems have the capability to produce an audit trail and activity logging to enable the assessment of the integrity of data and fraud detection.

Mandatory requirement 4

DETECT, RESPOND, RECOVER	*By improving business resilience and the ability to rapidly detect andrespond to Cyber Incidents or Cyber Crisis.*

4.1 Test the Cyber Incident Response Plan annually and report results to the Leadership Team and other relevant stakeholders, as required.

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

4.3 Report confirmed Cyber Incidents or Cyber Crisis to Cyber Security NSW.

4.4 Evaluate effectiveness of Cyber Incident Response Plan following a Cyber Incident or Cyber Crisis and identify and implement improvements.

4.5 Maintain a register of Cyber Incidents and Cyber Crisis to allow identification of patterns and trends and high-risk areas that need targeted risk treatment.

Mandatory requirement 5

REPORT	*By reporting against the requirements outlined in the Policy and other cyber security measures for the previous financial year.*

5.1 Provide status updates on control measures implemented for any cyber security risks classified as 'moderate', 'high', 'extreme' to each meeting of Council's Audit, Risk and Improvement Committee.

5.2 Report suspected or actual Cyber Incident or Cyber Crisis to the first ARIC meeting following the breach or after becoming aware of the suspected breach.

5.3 Provide statistical reporting on Cyber Incidents or Cyber Crisis concerning Council to the ARIC annually.

5.4 Provide reporting to the Leadership Team and ARIC (as required) regarding non-conformance with this Policy and Security Procedures.

1. Roles and responsibilities

- **Council staff, Councillors, contractors/consultants, and service providers** are responsible for:
  - Managing the risk associated with ICT systems and information and ensuring compliance with Policies, standards, procedures, and guidelines.
  - Reporting non-conformance with this Policy and/or suspected or actual Cyber Incidents or Cyber Crisis immediately to the ICT Manager.

- **Audit Risk and Improvement Committee** is responsible for overseeing and advising the General Manager and the Governing Body of:
  - appropriateness and/or effectiveness of internal controls, processes and procedures for the risk Council faces in relation to cyber security.
  - Compliance, or otherwise, of stakeholders with Council's policy and procedures for managing cyber security risk including reporting requirements.
  - Trends or patterns evidenced in the occurrence(s) of Cyber Incidents or Cyber Crisis.

- **ICT Manager** is responsible for:

    - Overseeing the implementation, adherence to and review of this Policy.
    - Defining and implementing an Information Security Incident and Data Breach Response Plan.
    - Developing a cyber security strategy, architecture, and risk management process and incorporating these, with the assistance of the Enterprise Risk Coordinator, intoCouncil's current risk management framework and processes.
    - Assessing and providing recommendations on any exemptions to this Policy and Security Procedures.
    - Attending ARIC meetings to assist in meeting reporting requirements, as required.
    - Taking the lead in investigating, responding to and reporting on suspected or actual Cyber Incidents and Cyber Crisis.
    - Reporting Cyber Incidents and Cyber Crisis to Cyber Security NSW and the ARIC.
    - Representing Council on whole-of-government collaboration, advisory or steering groups established by Cyber Security NSW.
    - Establishing training and awareness programs to increase employee cyber security capability.
    - Maintaining the register of Cyber Incidents or Cyber Crisis'.

- **Enterprise Risk Coordinator** is responsible for:

    - Assisting the ICT Manager in analysing cyber security risks
    - Ensuring the effectiveness of cyber security controls are reviewed as part of a Council wide program.

2. Definitions

ARIC - Audit, Risk and Improvement Committee.

Cyber Incident - moderate or higher impact to services, information, assets, reputation or relationships. Public visibility of impacts through service degradation or public disclosure of information/systems breaches, with economic impacts.

Cyber Crisis - major disruption to services and operations, with genuine risks to critical infrastructure and services, with risks to the safety of citizens and businesses. Intense media interest, large demands on resources and critical services.

ICT - Information and Communications Technology, includes software, hardware, network, infrastructure, devices and systems that enable the digital use and management of information and the interaction between people in a digital environment.

Security Procedures - Council's internal cyber security procedures including both functional and assurance requirements within a product, system, process, or technology environment.

Contact officer

ICT Manager.

Related documents

Policies

Code of Conduct
Privacy management policy
Risk Management Policy

Procedures

A number of procedures will be developed and will be approved by the General Manager and Leadership Team post adoption of this policy

Legislation

Privacy and Personal Information Protection Act 1998 (NSW)
Health Records and Information Privacy Act 2002 (NSW)
Government Information (Public Access) Act 2009 (NSW)
State Records Act 1998 (NSW)

Other

Australian Cyber Security Centre (ACSC) Essential 8:
https://www.cyber.gov.au/publications/essential-eight-explained

NSW Government Digital – 'Mandatory 25' Requirements for Cyber Security:
https://www.digital.nsw.gov.au/policy/cyber-security-policy/mandatory-requirements

Office use only	CM: D20/2822	Next review date: Annual	
Version	Purpose and description	Date adopted by Council	Resolution no.
0.1	Initial draft 14/09/2020		
0.2	Draft reviewed 27/01/2021		
0.3	Final review 30/08/2021		

Downloading and printing this document will produce an uncontrolled copy, which may not be current

Attachment 2

(Policy to be revoked)

POLICY	Records Management		
OVERVIEW	To provide a framework that outlines responsibilitiesfor the management and handling of records.		
AUTHORISED BY COUNCIL	ROUS	RRCC	FNCW
	18/06/2014	25/06/2014	24/06/2014
REVIEW DATE	30/06/2015		
FILE	172	843	1294

BACKGROUND

The purpose of this policy is to ensure that full and accurate records of all activities and decisions of Council are gathered, created, managed and retained or disposed of appropriately and in accordance with legislative requirements. This policy is designed to support Council to effectively and efficiently manage its records thereby enhancing and improving business operations, transparency and accountability. This Policy applies to all records in all formats, including electronic records and is in line with government policy on managing information as an asset.

POLICY

Definition

gathering information refers to the manner in which Council collects information through documents, databases other information sources and during the investigation of incidents.

Objectives of records management at Council

Council’s records management program is a planned, co-ordinated set of policies, procedures, people, systems and activities designed to ensure:

1. Appropriate records exist to support and facilitate Council operations and customer service.
2. Records are managed efficiently and can be easily accessed and used.
3. Records are stored as cost-effectively as possible and when no longer required they are disposed of in a timely, efficient and secure manner.
4. Records of long term value are identified and protected for historical and other research purposes.
5. Council is compliant with its legislative obligations and records management practices including the NSW Government’s objectives for recordkeeping.
6. Technology dependant records are maintained in an authentic and accessible form for as long as they are required.
7. The rights and interests of Council, its customers and the public are protected.
8. Evidence of actions and decisions and precedents for future decision making are documented.
9. Records are stored in a format which are admissible to a court of law as evidence.
10. Customer services are delivered in an efficient, fair and equitable manner.

Elements of Council’s records management program

- Creation and capture
  Records (both electronic and paper forms) are kept of decisions and actions made in the course of official Council business. Council’s records information management system is used to register records.

- Storage and Security
  Hardcopy records currently in use are securely stored in designated storage areas with access restrictions as appropriate for the file classification. Rarely used records or records no longer in use but still required to be retained are securely stored in a designated archive storage area.

  Electronic records are stored in a safe and secure manner as outlined in the *State Records Act 1998*, the *Privacy and Personal Information Protection Act 1998* and the *State Records Normal Administrative Practice* ('NAP'). Council ensures that electronic records are backed-up as per operational requirements.

- Maintenance and monitoring
  The location of each record is recorded and updated at every movement of the record. This ensures that records, as assets, can be accounted for in the same way that the other assets of Council are.

  Historical data is migrated into new systems within the means of Council.

- Disposal
  Council's records are covered under the *State Records Authority of NSW General Retention and Disposal Authority for Local Government*. No Council records are to be disposed of unless in accordance with this retention and disposal authority or the NAP provisions of the *State Records Act 1998*.

- Access
  Records must be available to all authorised staff that require access to them for legitimate Council purposes.

  Access to Council records by members of the public, including requests under the *Government Information (Public Access) Act 2009*, are handled in accordance with Council Procedure or as otherwise required by law.

Contractors and outsourced functions

Records created by contractors performing work for or on behalf of Council belong to Council, and are covered under the *State Records Act 1998*. This includes the records of contract staff working on the premises as well as external service providers. Contractors are to manage records that they create on behalf of Council according to the terms of their contract.

Responsibilities

Records management is a responsibility of every person within Council including the General Manager and Councillors. Managers and supervisors are responsible for ensuring effective records management within their respective areas of responsibility. All Council employees must:

- Create full and accurate records of Council activities, including records of all decisions and actions made in the course of official duties.
- Ensure that all records are provided to the Records Officer so that they can be captured into Council's recordkeeping systems.

In conjunction with the responsibilities outlined above, the IT Manager will be responsible for the:

- Back-up of server data; and
- Security of server, server data and back-ups thereof.

RELATED POLICIES

Information Communication Technology policy.

RELATED PROCEDURES

Tenders Procedure.
Gathering Information for Incident Management Procedure.

LEGISLATION

Copyright Act 1968 (Cth)
Evidence Act 1995
Government Information (Public Access) Act 2009
Health Records and Information Privacy Act 2002
Local Government Act 1993
Privacy and Personal Information Protection Act 1998
State Records Act 1998 – including standards and retention and disposal authorities issued under the Act

RELATED DOCUMENTS

Australian Standard, AS ISO 15489-2002, Records management.
Code of Conduct.
NSW Governments Recordkeeping Manual Guideline 8 – Normal Administrative Practice
Premier's Memoranda and Circulars, including C2003-17 and M2007-08.
Rous Water's Records Disaster Plan.

CONTACT OFFICER

Manager Governance
Records Officer
IT Manager.