IT AND CYBER SECURITY POLICY

Public Document

Version: 2 / ECM: ECM Document Set ID: 6433622

Adopted by: Council on 4 April 2023

Ownership: Corporate Services

TABLE OF CONTENTS

Purpose

To establish a basic and robust framework for the protection and use of information technology assets and resources within the business and provide adequate cyber security protections. This will assist in ensuring integrity, confidentiality and availability of Council's information, data and assets.

Objectives

1. To ensure any asset or resource that stores or accesses Council information or data including ICT, OT and IoT is secure. This includes but is not limited to:

    - computer systems, PCs, mobile devices, portable storage devices, telephonic systems and smart phones
    - other peripheral systems that use automated or remotely controlled or monitored assets such as parking technology, video surveillance, alarms and building management
    - hosting/cloud-based agreements and third-party ICT service providers/vendors

.

2. To support good cyber security culture, planning and governance in the organisation.

3. To properly manage cyber security risks and safeguard and secure Council's information and systems.

4. To improve Council's resilience to cyber-attacks and crime including its ability to rapidly detect cyber incidents and respond appropriately.

5. To minimise the impact of incidents on the Council's image, reputation, business operations and profitability.

6. To ensure compliance with regulatory requirements.

7. To protect information so as to minimise the risk of financial and other loss to the Council.

8. To establish the accountability for employee actions in regards to protecting, disclosing, accessing, destroying and modifying Council information.

9. To support the strategic endeavours of Council by being safe, secure and reliable.

Scope

1. This policy is applicable to the whole of Council, its employees, contractors, consultants, and any other party given access to Council information technology assets or confidential information, including hosting/cloud-based agreements and third-party ICT service providers/vendors.

2. This policy applies to all information technology and physical assets that are owned or leased by Council or in Council's custody and control, and to Council confidential information.

Document Set ID: 6433622
Version: 2, Version Date: 06/04/2023

Areas of responsibility

1. The General Manager is responsible for overseeing the implementation, adherence to and review of this policy including the governance of ICT, OT and IoT.

2. System and information owners are responsible for managing the risk associated with relevant systems and information and ensuring compliance with policies, standards, procedures and guidelines. They are also responsible for reporting non compliances and associated actions to the Manager IT Services.

3. All Council permanent and temporary employees, contracted staff, consultants and other workers are responsible for ensuring personal compliance with this policy and related standards and procedures.

Exemptions

1. The General Manager is responsible for approving and monitoring all exemptions to the policy.

2. Exemptions to this policy must be recommended to the General Manager by the Manager IT Services who will ensure that the channel, system or information owner understands, acknowledges and accepts the risk associated with the exemption.

Discipline

1. Where a breach of this security policy is identified, whether accidental or intentional, individual users, system and information owners are required to notify the Manager IT Services immediately who will in turn notify the General Manager and all relevant stakeholders as appropriate.

2. Any breach of this policy by staff will be handled within the Council's governance framework for human resources.

IT and Cyber Security Standards

This overarching Policy (incorporating the IT and Cyber Security Standards (the Standards) which must be read in conjunction with this Policy) are the key contributors to the governance framework for IT and cyber security within Council. The Standards:

- address the need to protect confidential and sensitive information from disclosure, unauthorised access, loss, corruption and interference and is relevant to information in both electronic and physical formats
- are set out by category of user or responsibility – either User, Management or Technical
- are referenced to international (ISO) and local (ASD 8) standards to assist Council in ensuring its meets internal compliance objectives and adheres to best practice cyber security standards
- provide links to procedural documentation
- provide a security and acceptable use framework for Council
- help protect the assets of the Council
- provide a uniform level of control and guidelines for management
- (and this Policy) provide one IT security message to all
- advise what the IT security and acceptable use controls and guidelines are

The Standards are accessible in-house only via Council's Intranet. The Standards are a set of generic Standards developed and maintained by a cyber security vendor which are adapted to align with Council practices. The Standards are reviewed by the vendor on a monthly basis to ensure they are current and mapped to standards and mitigation strategies, thereby creating efficiencies in comparison to the alternative of maintaining Standards in-house. All amendments to the Standards proposed by the vendor are reviewed and approved by the Manager IT Services prior to the Standards system on the Intranet being updated. This provides effective control on content changes and applicability to Council's practices.

IT and Cyber Security Policy Statements

The Standards are concerned with what Council should do to protect its information and systems from significant risks and address all areas of IT and cyber security. However, policy Statements are annunciated in addition to the provisions of the Standards, in order promote and nurture the significance of IT governance.

Council will use all endeavours to adhere to the Standards and Statements set out in this policy. Council's abilities and reach in relation to IT governance matters are subject to those limitations imposed by the lack of resources available to an organisation the size of Council. This policy should be read in this context.

1. This Policy and access to the Standards be available to, understood, formally accepted and adhered to by all Council staff.

2. All Council staff have a responsibility to protect Council and to minimise the risk that might result from inappropriate use of such information.

3. Security standards and procedures be developed and reviewed as agreed with the cyber security vendor engaged by Council to ensure they continue to support the objectives of this policy.

4. All information technology and physical assets be secured in accordance with the relevant information security standards and procedures.

5. Council assets are to be made available to authorised people only, according to least privilege, and only be used in accordance with the relevant security standards and procedures. Access will be approved by managers.

6. All Council information rated confidential or internal use only be protected against intentional or unintentional access or disclosure.

7. All Council information and systems be protected and maintained to ensure that integrity is assured.

8. All Council information and systems be protected and maintained to ensure that availability is assured.

9. All access to Council information and systems be auditable to ensure accountability and non-repudiation of actions.

10. Defence in depth be applied to the design, development and deployment of all Council systems to ensure a balanced security approach.

Document Set ID: 6433622
Version: 2, Version Date: 06/04/2023

11. The design, development, deployment, and maintenance of systems be done in consultation with the Manager IT Services and in accordance with the security standards and procedures.

12. All Council systems and services comply with relevant national and international standards identified by the Manager IT Services.

13. Security incident management response procedures be implemented.

14. Information security risks and exemptions be included in the risk management framework and reviewed at annually or as otherwise reasonably practicable.

15. Council operate an achievable Information Security Management System (ISMS) to provide a systematic and repeatable approach to minimising information security risks, support cyber resilience and reduce the impact of security incidents.

16. Council develop and implement the ACSC Essential 8 where achievable.

17. Council has adopted and maintains an IT Strategy that details five key strategic principles that Council would adhere to when making investments into business systems and infrastructure implementations. These strategic principles and inherent mapping of software status be adhered to when Council updates its ongoing program of renewal and upgrade of technologies and considers system development life cycle, to ensure existing systems are within the Council's cyber risk tolerance.

18. Council ensure that new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including processes for internal fraud detection.

19. Council develop, implement and maintain a Cyber Security Plan that is integrated with Council's Business Continuity Plan framework. The Cyber Security Plan will work concurrently with Council's Business Continuity Sub-Plan for DCS IT Services and will address threats, risks and vulnerabilities that impact the protection of Council's information, data, assets and services. It will also consider cyber security threats when performing risk assessments.

20. Council investigate, develop and implement any achievable:

    - vendor monitor processes to ensure that vendors continually comply with the security requirements stipulated under this Policy and Council's IT Corporate Practices.
    - cyber security awareness and training program for all employee, contractors and ICT service providers that includes induction and ongoing refresher training.
    - processes that ensure cyber security risk management is embedded within non-IT management decisions.

21. Council share information on security threats and intelligence with Cyber Security NSW and cooperate across NSW Government to enable management of government wide cyber risk.

22. Council backup important new or changed data, software and settings on a daily basis. Restoration will be tested at least annually and when IT infrastructure changes.

23. Access Management

1. Access Management is the process of identifying, tracking, controlling, and managing user access rights to information systems. Any user who requests access to systems, applications, or data, will have their identity authenticated.

2. Council mandates requirements for access management controls across its technological environment to aid in managing access to its information systems.

3. Access to Council's IT systems be managed in a manner that maintains the confidentiality, integrity, and availability of Council's resources, and in a manner that complies with applicable legal and regulatory requirements.

4. Access granting, modification, revocation and ongoing access reviews for all applications and systems are mandated to ensure that users of Council's applications and systems who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening. It also ensures that access is removed when no longer required or when staff are terminated.

5. The IT system privileges of all users, systems, and independently operating programs be restricted based on the job function or need-to-know. This means that privileges must not be extended unless a legitimate business-oriented need for such privileges exists.

6. The Council's applications and systems will restrict access to the computers that users can reach over the Council's networks. These restrictions can be implemented via routers, gateways, and other network components.

7. User access be further restricted following the principle of least privilege, and in alignment with Council's delegations and applicable segregation of duties.

8. User account provisioning include creation of unique credentials for new users and disablement and revocation of a terminated user's access privileges upon termination.

9. Privileged access only be provided to users as needed. Users with privileged user accounts also have an organisational user account, which follows the principle of least privilege, and will use this organisational user account for their day-to-day job functions.

10. Privileged user accounts only be used when elevated privileges are required by the system or application.

11. Where there is a requirement for shared usage of an account this will be signed off by the Manager IT Services and relevant Directors and all usage will be traceable to an individual authorised user account.

12. All remote access to the Council's network utilise a secure solution, which employs multi-factor authentication, and a secure network encryption protocol.

24. Classification of information and systems

1. Council classify information and systems according to their business value. This involves consideration of such things as the impact of loss of confidentiality, integrity or availability.

2. Council adhere to *NSW Government Information Classification Labelling and Handling Guidelines* and assign responsibility for information asset protection and ownership,

implement controls according to their classification and relevant laws and regulations, and to identify the Council's "crown jewels".

3. Council's Records and Information Management Policy and Records and Information Management Strategy address the Guidelines' information and "crown jewels" requirements. The Council's "crown jewels" are identified and listed as Council's Vital Records in the Records and Information Management Strategy.

4. Council's IT Strategy addresses Guidelines' systems requirements.

5. Council ensure that its policies and strategies adhere to the Guidelines.

25. Cyber incident detection and response

Council strives to improve its resilience to cyber-attacks and crime including the ability to rapidly detect cyber incidents and respond appropriately. It aims to achieve this by:

1. developing and implement an incident response plan that is integrated with Council's Business Continuity Plan.

2. ensuring the incident response plan is tested at least annually and involves senior staff responsible for media and external communications.

3. ensuring the incident response plan is tested further by participating in or observing state-wide initiated security exercises.

4. reviewing security architecture and the IT Strategy with a view to implementing other monitoring tools and software for adequate logging of system activities where achievable.

5. reporting cyber security incidents to the Manager IT Services and/or Cyber Security NSW. The Manager IT Services will report periodically to the General Manager in this regard or in instances of serious incidents.

Definitions

ACSC Essential 8 means the list of mitigation strategies suggested by the Australian Cyber Security Centre (ACSC) for organisations to strengthen their cyber security controls. These consist of strategies to:

- mitigate the risk of malware delivery and execution
- limit the extent of cyber security incidents
- recover data and system availability

These strategies may also be known as **ASD 8** which means the Australian Signals Directorate (ASD) 'Essential 8' strategies. The ACSC is based within the ASD.

Council means Mosman Municipal Council.

Information Communication Technology (ICT) means Information Communication Technology all communication technologies, including the internet, wireless networks, cell phones, computers, software, middleware, video-conferencing, social networking, and other media applications and

services enabling users to access, retrieve, store, transmit, and manipulate information in a digital form.

Information Security Management System (ISMS) means security management based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

I**nternet of Things (IoT)** means physical objects that containing embedded technology used to communicate, sense or interact with their internal states or the external environment using computer networks. Examples of Council IoT include parking technology, video surveillance, alarms and building management.

IT and Cyber Security means:

- Confidentiality - information must not be made available or disclosed to unauthorised individuals, entities, or processes
- Integrity - data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes
- Availability - information must be accessible and useable on demand by authorised entities

Operational Technology (OT) means hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

Related Information

1. Mosman Council IT Corporate Practices accessible at http://itcorporatepractices.mosman.council/index.html comprising:

    - User Standards
    - Manager Standards
    - Technical Standards

2. *NSW Cyber Security Guidelines – Local Government* (by Cyber Security NSW, July 2021)
3. *NSW Government Information Classification Labelling and Handling Guidelines*
4. Australian Cyber Security Centre (ACSC) Essential 8
5. Mosman Council Business Continuity Sub-Plan - DCS IT Services (May 2021)
6. Mosman Council Cyber Incident Response Plan (to be developed)
7. Mosman Council Cyber Security Plan (to be developed)
8. Mosman Council IT Strategy
9. Mosman Council Information Technology Governance Corporate Practice
10. Mosman Council Internet and Mobile Computing Corporate Practice
11. Mosman Council Records and Information Management Policy
12. Mosman Council Records and Information Management Strategy

Review

This policy will be reviewed every two years unless otherwise directed by the Executive team to ensure ongoing compliance with legal and industry requirements.

Document Set ID: 6433622
Version: 2, Version Date: 06/04/2023

Contact

Enquiries should be directed to the Manager IT Services on 9978 4015.

Amendments

Date	Amendment	Reference
11 March 2019	Internal policy adopted by General Manager	-
4 April 2023	Reviewed to address recommendations in Internal Audit Report on Cyber Security dated June 2022 and to present to Council to adopt as public policy.	CS/7