IPSWICH CITY COUNCIL

Information Systems Security (InfoSec) Policy

Version Control and Objective ID	Version No: 0.1 (Draft)	Objective ID: A5885002
Approved by Council on		
Date of Review		

1. Statement

Council will establish and maintain an Information Security Management System (ISMS) that provides for appropriate security and confidentiality of information, information systems, applications and networks owned, leased or operated by all Council users, operations and entities as required to address corporate risks and to satisfy regulatory requirements.

2. Purpose and Principles

This policy guides Council's approach to managing the security of all digital information captured in and managed by information systems used across council. The following principles and requirements underpin Council's commitment to InfoSec:

Policy Aspect	Requirement
Information Security Planning, Capability and Risk Management	Council will establish an Information Security Management System (ISMS), approved by the ICT Steering Committee, to manage Council's InfoSec risks. The ISMS will detail: a. InfoSec goals and strategic objectives of Council, including how InfoSec management intersects with and supports broader business objectives and priorities b. Threats, risks and vulnerabilities that impact the protection of Council's ICT Assets c. Council's tolerance to InfoSec related risks d. Council's capability and capacity to manage and develop InfoSec Controls e. Council's strategies to implement and maintain the ISMS, maintain a positive risk culture and deliver against this Policy.
ISMS Administration and Reporting	Matters relating to the routine operation, administration and evolution of Council's ISMS will be overseen by the Manager ICT Branch (CIO). ISMS matters requiring escalation will be taken, in the first instance, to the ICT Steering Committee for consideration and direction. InfoSec Risks will also be captured, reported and tracked within the Council's Risk Management Framework. The ICT Steering Committee will provide a bi-annual report on the ISMS to the Audit and Risk Committee on: a. The security outcomes supported by the ISMS b. The maturity of the capability identified in the InfoSec Framework c. Key risks to Council's ICT Assets d. Details of measures taken to mitigate or otherwise manage identified security risks
InfoSec Governance for Contracted Service Providers	The requirements of this Policy apply equally to ICT Assets procured directly or included indirectly as part of any broader outsourcing of business services. Each Business System Owner is accountable for the risks arising from ICT Assets procured as a component of broader business outsourcing.

Policy Aspect	Requirement
Sensitive and Classified Digital Information	Council will: a. Identify and classify Digital Information developed and used across Council for the purpose of defining and enforcing appropriate InfoSec Controls b. Assess the sensitivity and security classification of Digital Information holdings c. Implement proportional InfoSec Controls for Digital Information reflecting the value, importance and sensitivity
Proportional InfoSec Controls	Council will define and enforce InfoSec Controls based on the Risk exposure associated with the loss or compromise of any given ICT Resource. In determining InfoSec Controls to be applied Council will consider: a. **Confidentiality:** Risk associated with unauthorised access to any given ICT Resource and ensuring that ICT Resources are only accessible to those with authorised access b. **Integrity:** Risk associated with the accuracy and completeness of Digital Information and processing methods c. **Availability:** Risk associated with the loss of availability, or degraded performance of ICT Resources
Safeguarding Information from Threats	Council will, as a minimum, mitigate common and emerging InfoSec threats based on the Australian Cyber Security Centre "Essential Eight" controls: a. Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers. b. Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate. c. Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications. d. User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers. e. Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing. f. Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository. g. Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions. h. Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes. Council will adopt or extend further InfoSec Controls as necessary to safeguard information as informed via structured risk assessments.

Policy Aspect	Requirement
Access to ICT Resources	Council will enforce access controls to ICT Resources. This includes: a. Ensuring that System Users who access sensitive or classified Digital Information have appropriate authorisation and continuing need to access that Information b. Controlling access to supporting ICT Assets and Services (networks, remote access, infrastructure and applications etc), both on-premise and cloud hosted c. Periodic audit of System User access and activity to ensure appropriate and reasonable access to ICT Assets
InfoSec Controls Across ICT Asset Lifecycle	Council will ensure InfoSec Controls are properly considered, implemented and maintained across the operating lifecycle of all ICT Assets including: a. Sensitive and classified information is identified, and appropriate InfoSec requirements are addressed in the specifications, analysis and/or design phases for new ICT Assets b. Where the ICT Asset is procured 'as-a-service', all requirements of this policy are considered with required controls reflected in the service contract c. InfoSec Controls are established and validated during all stages of System development, as well as when new Systems are implemented and maintained in the operational environment d. Appropriate change control, acceptance and system testing, planning and migration control measures are carried out when upgrading or installing software in the operational environment e. A patch management program for operating systems, firmware and applications of all ICT Assets is implemented to maintain vendor support, increase stability and reduce the likelihood of threats being exploited

3. Strategic Plan Links

This policy relates to:

- Strengthening our local economy and building prosperity
- Managing growth and delivering key infrastructure
- Listening, Leading and Financial Management

4. Regulatory Authority

- QGCIO Information Security Policy (IS18:2018)
- Public Records Act 2002
- Right to Information Act 2009
- Information Privacy Act 2009
- Local Government Act 2009

5. Scope

This Policy applies to internal Business System Owners, System Users and Risk Owners, not external customers and users of Council operated or supplied ICT Assets, Resources and Services.

External users (eg Citizens, Business etc) of Council's ICT Assets will be subject to terms and conditions unique to each offered service.

6. Roles and Responsibilities

Role	Responsibilities
Information Security Officer (ISO)	• Develop and maintain ISMS • Provide stakeholders with advice, guidance and services related to InfoSec • Review and approve InfoSec Controls for individual Information Assets • Establish, review, track and report on waivers and deviations issued against non-compliant Information Assets • Own and direct the development of InfoSec Controls the have enterprise applicability
ICT Strategy, Enterprise Architecture and Governance Manager	• Ensure appropriate governance across ISMS • Ensure coherent and structured architectural approach to InfoSec Controls
Manager ICT Branch (CIO)	• Owner of this Policy • Sponsor/owner of ISMS • Sponsorship and promotion of Governance of ISMS and InfoSec Risk Management
ICT Service Delivery Manager	• Routine operation and management of ICT Assets and InfoSec Controls
Records and Knowledge Manager	• Identify and classify Digital Information across all Council Information Assets • Review the Digital Information managed within any new ICT Asset undergoing procurement and implementation and provide advice to the Business Application Owner and the ISO on information sensitivity and security classification
Corporate Risk and Planning Manager	• Provide advice, interpretation and direction on InfoSec related risks and relevance/alignment with wider Council Risk Management Framework
ICT Steering Committee	• Review and provide advice and directions • Support/sponsor investment into InfoSec Controls required to achieve ISMS outcomes
Business System Owner	• Complying with this policy, the procedures, and applicable technical standards that extend on this Policy • Managing InfoSec risks associated with ICT resources and third party service providers under their remit; • Sponsoring and directing the development, implementation and maintenance of InfoSec Controls for ICT Assets under their remit, in accordance with the Risk Management Framework and applicable technical standards
System Users	• All System Users shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

7. Key Stakeholders

The following will be consulted during the review process:

- ICT Steering Committee
- Business System Owners

8. Monitoring and Evaluation

- Ageing and resolution of InfoSec related Departures and Waivers issued for non-compliant ICT Assets
- Effective identification and resolution of InfoSec Incidents as reported by SIEM
- Effective reporting and awareness of ISMS to both ICT Steering Committee and ARC
- Strategic and Operational Risks related to InfoSec exposure and Controls within tolerance
- Number of information security breaches related to non-compliance with ethical and professional behaviour guidelines
- Frequency of independent reviews of governance of information security
- Frequency of information security reporting to the ICT Steering committee
- Number of external/internal audits and reviews

9. Definitions

Term	Definition
Business System Owner	A person with primary accountability for the business outcomes and functions provided by a Council ICT Asset, including ownership and accountability for any associated InfoSec risk.
InfoSec	Information Security (InfoSec) is a set of related strategies, processes, tools and policies that collectively identify, classify, prevent, counter and recover from threats to ICT Resources.
InfoSec Control	Any contractual, management, operational or technical measure (including safeguards or countermeasures) put in place for the purpose of enabling and enforcing InfoSec.
InfoSec Incident	Any event that may adversely impact the confidentiality, integrity or availability of a Council ICT Resource.
Digital Information	Information that is in a digital or electronic form and is stored, processed or transmitted within an ICT Resource.
ICT	Information and Communications Technology that enables or supports Council owned or operated business, operating departments or services.
ICT Asset	Hardware, software, cloud-based services, communication devices, data centres, or networks that are owned, leased, leveraged or operated by Council.
ICT Resource	Any ICT Service, ICT Asset or Digital Information.
ICT Service	Any business or technology function provided using one or more ICT Assets, including, but not limited to: • application systems (including software-as-a-service); and • ICT infrastructure services such as operating systems, databases, voice and data telecommunications services, network services, media services, file and print services, and email services.
ISMS	An Information Security Management System (ISMS) is a cohesive and planned suite of policies, procedures, roles and InfoSec Controls for systematically protecting an organisation's ICT Resources. The goal of an ISMS is to minimise risk and ensure business continuity by pro-actively addressing known InfoSec risks and limiting the impact of any InfoSec Incident.
Risk	Has the meaning provided in the Risk Management Framework 2019.
System User	Any Council employee, volunteer, contractor or elected official that is provided with access to Council provided ICT Resources.

10. Policy Owner

This Policy is owned by ICT Branch Manager.