City of Greater Geraldton

4.6 INFORMATION SECURITY MANAGEMENT SYSTEM

SUSTAINABILITY THEME

Leadership

OBJECTIVES

To set out a framework and approach to Cyber and Information Security at the City of Greater Geraldton (City) to ensure the confidentiality, integrity, and availability (CIA) of all City information assets and resources.

For the purposes of this policy, Information Security is the umbrella term which includes Cybersecurity and any other security topics.

POLICY STATEMENT

This policy applies to all City employees, contractors, and volunteers.

This policy applies to all people, processes and technology which utilise or interact with the City's people, processes, and technology.

POLICY DETAILS

1. Organisations face considerable and persistent threats to their information systems. The City values its information assets and those entrusted to it, and is committed to the effective governance of enterprise IT (GEIT).
    1.1 The City will develop and implement an Information Security Management System (ISMS) to provide a systematic and repeatable approach to minimise information security risks, support cyber resilience and reduce the impact of security incidents.
        1.1.1 The City will follow established frameworks, standards, and industry best practice in its development and implementation of the ISMS.
        1.1.2 The City will utilise the City's Risk Management Framework to assess information security risk.
        1.1.3 The City will adhere to current, and be aware of emergent, legal, statutory, regulatory, and contractual requirements in the implementation of the ISMS.
2. The ISMS will encompass an Executive Management Team (EMT) endorsed Information Security Strategy supported by Plans, Policies, Standards, and Procedures (artefacts).
    2.1 The artefacts developed within the ISMS will be guided by the following key principles:
        2.1.1 Confidentiality – to ensure that information is only accessed by the intended parties and is protected from unauthorised access or dissemination.
        2.1.2 Integrity – to ensure that information is kept whole and accurate throughout its entire lifecycle.
        2.1.3 Availability – to ensure that information and information systems are available and operational when they are required.

2.1.4 Need-to-know – information is only to be made available to those persons that have a genuine need to access the information in order to perform their duties.

2.1.5 Least-privilege – access to information is to be granted with the minimum access privileges necessary for the user to perform their duties.

2.1.6 Non-repudiation – to ensure that an individual does not have the ability to deny the actions they took on the City's information systems.

2.1.7 Separation of duties – the ability to perform critical functions shall be split across multiple employees to reduce the potential for misuse of a process or system.

2.1.8 Continual Improvement – to ensure that a journey of continual review and improvement of security practices is incorporated in current operations and future planning.

3. The City understands that for information security to be at its most effective that it must become a part of the culture of the organisation and the people that interact with it.

   3.1 The City will continue to educate employees, contractors, and volunteers with promotion of the ISMS.

   3.2 The City will aspire to extend its ISMS to educate and support the wider community, and seek to collaborate with government, industry, and academia. In turn, learn from others.

4. The City will provide adequate budget and appropriate resources to develop, implement and maintain the ISMS.

   4.1 Funding opportunities will be investigated when available.

KEY TERM DEFINITION

Information Security refers to the processes and practices used by organisations to protect their data.

Cybersecurity is the activity of securing computer systems, networks, devices, and application from cyber-attack. It is a sub-set of Information Security.

Information Security Management System is a holistic approach to information security management based on a business risk approach, to establish, implement, monitor, review, maintain and improve cyber and information security.

ROLES AND RESPONSIBILITIES

Chief Executive Officer

- Ensure that security policy is in place and a security aware culture is established.
- Provide the audit committee with regular reports on the functioning of the ISMS.

Executive Management Team

- Provide leadership and ensure that a security aware culture is promoted through training, strategies, business plans and projects.
- Ensure an appropriate level of resources is available, or Council is made aware of the need for additional resources, to implement the ISMS.
- Ensure that all systems have an information asset custodian identified.
- Ensure information security objectives and principles are taken into account during the decision making process.

Manager ICT Services

- Develop and implement the ISMS.

- Plan and transition to the states of security maturity and ensure alignment to overall business needs and enterprise architecture.
- Perform annual reviews of the ISMS.

Managers

- Ensure staff comply with the ISMS artefacts and complete relevant training or information sessions.

Senior Cybersecurity Engineer

- Design security architecture and implement security systems and processes.
- Lead investigations into alleged information security breaches.

Employees, Contractors and Volunteers

- Complete all assigned security training in a timely manner.
- Notify security team of security risks, incidents and breaches in a timely manner.

WORKPLACE INFORMATION

Local Government Act 1995

Privacy Act 1988

Community Strategic Plan 2021-2031

Corporate Business Plan

ICT Strategic Plan

Strategic Internal Audit Plan

CGG Risk Management Framework

Council Policy 4.7 Risk Management

Council Policy 4.24 Risk Appetite and Tolerance

ISO/IEC TS 27022:2021 Guidance on Information Security Management System Processes

ISO/IEC TS 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements.

POLICY ADMINSTRATION

Directorate		Officer	Review Cycle	Next Due
Corporate and Commercial Services		Manager ICT Services	Biennial	2024
Version	**Decision Reference**	**Synopsis**		
1.	CCS XXX 00/00/2022	New Policy		