Information Security Policy

CITY OF GOLDCOAST.

DETAILS

Council ☒ **Admin** ☐

Effective from:		3 March 2020
Contact officer:		Policy Officer, Business Innovation and Technology Services
Next review date:		March 2022
File reference:		IM634/171/03(P4)
iSpot #	This policy	23526603
	Value Proposition	41643605

OBJECTIVES AND MEASURES

Objectives	• Council of the City of Gold Coast (Council) must ensure the confidentiality, integrity and availability of all information. • Identify, assess and manage Information Security risks. • Information security management complies with legislation and contractual obligations.
Performance measures	• Number of untreated, intolerable information security risks present in Corporate and Directorate risk registers. (Target is zero) • Number of legislative and contractual breaches relating to Information Security. (Target is zero)
Risk assessment	High

POLICY STATEMENT

Information is a strategic asset which underpins many functions of Council and the security of this information is crucial in delivering efficient, effective and innovative services to the community.

Information security is the responsibility of all employees. Roles and responsibilities are defined in Appendix A.

Compliance with the Information Security Policy and associated Standards is mandatory. Where it is not practical or economically viable to meet a requirement of the Information Security Policy or a supporting standard, exceptions are subject to the approval by the Chief Information Officer (CIO).

This policy and its related standards direct that:

1. Information security risks must be assessed, raised and managed through established risk management processes by Information Asset Custodians.

2. All Councillors and employees have an obligation to understand the value and sensitivity of information and to manage in accordance with the Information Security Classification Standard.

3. All Councillors and employees must not release information that they know, or should reasonably know, is confidential to Council by any means including information communicated via voice/video/text messaging, email and social media accounts.

4. All Councillors and employees have an obligation to report information security breaches or suspected information security breaches in accordance with Information Security Incident Management Standard.

5. Security incident management responsibilities and procedures must be established by Information Asset Custodians to ensure an effective and efficient response to information security incidents in accordance with the Information Security Incident Management Standard.

6. Council must operate an 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.

7. Employees responsible for information assets must identify information security risks in accordance with the Information Security Risk Management Standard.

8. Information Asset Custodians are responsible for the effective implementation of controls that are aligned with this policy and associated standards. For assistance completing Information Security risk assessments contact the Executive Coordinator Cyber Security and Information Solutions or your directorate risk representative.

SCOPE

This policy applies to all information and information assets supporting Information Communication Technology (ICT); Operational Technology (OT) and Internet of Things (IoT) assets that are owned, managed or operated by Council.

The physical security of information is outside of the scope of this policy and described in the Protective Security Policy. Physical security provides a safe and secure physical environment for Council employees, information and assets.

DEFINITIONS

Terms	Meaning
Confidential Information	Information restricted to authorised users on a 'need to know' basis, including for internal or public release.
Council	Council of the City of Gold Coast
Cyber Security	Cyber security is the combination of people, policies, processes and technologies employed by an enterprise to protect its assets. While 'Cyber' generally refers to technology aspects of Information Security, in the Council context the term 'Cyber Security' is interchangeable with 'Information Security'.
Information	A collection of data or documents processed, analysed, interpreted, organised, classified or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium (including electronic (digital), print, audio, video, image or graphical form).
Information Asset	A collection of data stored in any manner and recognised as having value for the purpose of enabling the Council to perform its business functions, thereby satisfying a recognised Council requirement.
Information Asset Custodian	As defined in Council's Information Management Policy, a custodian of an information asset is responsible for ensuring corporate information is collected and maintained according to specifications and priorities determined by consultation with the user community, and made available to that community and in a format that conforms with Council's standards and policies.

Terms	Meaning
Employee	As defined in Council's Code of Conduct policy, the term Employee includes all Gold Coast City Council employees, regardless of their employment status, role or position - permanent, temporary, casual or part-time employees, Agency Resources or volunteers, managers, direct supervisors, team members or individuals. The term 'Employee' is interchangeable with the terms of 'Workforce' or 'Staff'.
Information Communication Technology (ICT) Information Security Incident	Where a risk is realised and potential exists for compromise of business operations or information security requiring a business response.
Information Security Risk	Information security risk analyses and manages threats and vulnerabilities associated with the operation and use of information and the environments in which systems operate which may result in business impacts through loss of confidentiality, integrity or availability of information.
Information Security Management System (ISMS)	Security management based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
Internet of Things (IoT)	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 safety cameras, flood level sensors, bin and BBQ gas sensors.
Intolerable Risk	A level of risk which cannot be tolerated. See Corporate Risk – Consequence & Likelihood Table, Risk Matrix and ALARP Table (iSpot # 37777186).
Operational Technology (OT)	Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events. Examples of Council OT include SCADA systems.
Portable Storage Device	A portable storage device (PSD) is a small hard drive designed to hold any kind of digital data. Examples include Laptops, Tablets, Mobile Phone, USB flash drive.
Security Specialist	A security specialist can be defined as anyone that specialises in the security of people, assets, networks, telecommunications systems, and IT systems.
System Administrator	An individual who is responsible for overseeing the day-to-day operability of a computer system or network. This role normally carries special privileges including access to manage the protection state and software of a system.

See Information Security Policy – Definitions (iSpot #72862295) for a complete list of definitions used in the Information Security Policy and supporting standards.

SUPPORTING DOCUMENTS

Related Standards

The Information Security Policy is supported by a range of mandatory standards. These are further explained within Appendix B.

Information Security Access Management Standard (iSpot #74171314)
Information Security Classification Standard (iSpot #74164641)
Information Security Incident Management Standard (iSpot #74163881)
Information Security Risk Management Standard (iSpot #74582096)
Logging and Monitoring Standard (iSpot #74171023)
Patch Management Standard (iSpot #74164443)
Remote Access Standard (iSpot #74171277)
Secure Disposal and Sanitisation Standard (iSpot #74431949)
Supply Chain Security Standard (iSpot #74163162)
Vulnerability Management Standard (iSpot #74170892)

Related Documents

Enterprise Risk Management Framework (iSpot #29129462)
Enterprise Risk Management Manual (iSpot #37282382)

Appendix A: Roles and Responsibilities
Appendix B: Information Security Standards

RELATED POLICIES AND DELEGATIONS

Audit Committee Policy
Business Continuity and Internal Incident Management Policy
Code of Conduct for Employees Policy
Delegated Power and Authorisations Policy
Digital City Data Policy
Disciplinary Policy
Enterprise Risk Management Policy
External Communication Policy
Expenses Reimbursement and Provision of Facilities for Mayor and Councillors Policy
Fraud and Corruption Control Policy
ICT Resource Usage Policy
Information Management Policy
Information Privacy Policy
Portable and Attractive Items Policy
Procurement Policy and Contract Manual
Protective Security Policy
Recruitment Selection and Appointment Policy
Right to Information and Information Provision Policy

Delegation DE01407
Delegation DE02377

LEGISLATION

Crime and Misconduct Act 2001
Electronic Transactions (Queensland) Act 2001

Evidence Act 1997
Information Privacy Act 2009
Local Government Act 2009
Public Interest Disclosure Act 2010
Public Records Act 2002
Public Sector Ethics Act 1994
Right to Information Act 2009
Workplace Health and Safety Act 2011
Cybercrime Act 2001
Spam Act 2003
Telecommunication Act 1997
Security of Critical Infrastructure Act 2018
Work Health and Safety Regulation 2011

RESPONSIBILITIES

Sponsor	Director Organisational Services
Owner	Chief Information Officer

VERSION CONTROL

Document	Date	Approved	Amendment
23526603 v6	03.03.20	ETG20.2027.007/G20.0303.029 & iSpot #75885472	Major amendments
23526603 v5	19.08.16	GA16.0125.007/G16.0129.008	Major amendments
23526603 v4	12.12.14	GA14.1209.012/G14.1212.015	Council approval
23526603 v3	16.09.13	GA11.1012.001/G11.1017.014	Council approval
23526603 v2	26.10.11	iSpot #30835825	Minor change
23526603 v1	15.02.11	CGC07.0704.009	iSpot #30505544

Chief Executive Officer (CEO)

a. ensure that security policy is in place and a security aware culture is established,
b. approve minor changes to this policy.

Chief Operating Officer (COO)

a. make recommendations to the CEO in the approval of major changes to this policy,
b. approve minor changes to this policy,

Director Organisational Services (DOS)

a. approve major changes to Information Security Standards, which change the intent or impact the governance of the policy, that do not apply to Councillors.

Chief Information Officer (CIO)

a. coordination, communication, and implementation of this policy,
b. provide advice on Information Security Policy,
c. ensures coordination of corporate policy awareness and implementation,
d. establish, endorse and maintain standards, specifications and controls for the secure design, implementation, management and disposal of information systems and equipment,
e. maintain a register of all standards relating to the Information Security Policy,
f. provide exemptions to this policy and associated standards,
g. maintain a register of exceptions to this policy and associated standards,
h. establish the Security Incident Response Team and Security Incident Management,
i. approves minor changes to Information Security Standards that do not change the intent or impact the governance of the policy,
j. maintain version history / version control of all changes to Information Security Standards.

Executive Coordinator Cyber Security and Information Solutions

a. recommends changes to this policy and supporting documentation, policy implementation, maintenance and the application of information security as part of the Council's Cyber Security Plan,
b. responsible for establishing and chairing the ISMS committee and reporting to senior leadership,
c. responsible for the performance of information security risk assessments,
d. facilitates information security risk assessments,
e. leads investigations into alleged Information Security breaches that are not likely to result in official misconduct proceedings,
f. leads the implementation and operation of Council wide information security systems and processes,
g. monitors and reports on compliance and performance as required,
h. is responsible for the provision of advice regarding confidentiality maintenance on external information provided to Council,
i. leads Security Incident Response Teams when the CIO is unavailable.
j. provides support and advice to employees requiring assistance in the identification, assessment and treatment of risks, incidents and breaches.

Directors

a. provide leadership, and within their Directorate, ensure directorate strategy is in place, and that a "security aware" culture is promoted through corporate and on the job training,
b. ensure that all systems have an information asset custodian identified and recorded in the Configuration Management Database (CMDB),
c. co-operate with the CIO to support the implementation of the Information Security Policy,
d. notify the BITS Executive Coordinator Business Engagement to update the Information Asset Register with any changes in Information Asset Custodians,

e. ensure that an appropriate level of resources is available, or Council is made aware of the need for additional resources to implement security controls that manage information security risks.

Managers

a. ensure that staff under their direction comply with the Information Security Policy and attend relevant training or information sessions,
b. ensure that all adopted standards and procedures relevant to their staff, business functions and services, are implemented with their branches,
c. responsible for disciplinary matters resulting from the findings of information security breach investigations. This excludes matters that may result in official misconduct proceedings.

Manager Corporate Assurance

Ensure compliance to standards referred to in the Information Security Policy on a risk-based rotational basis.

Executive Coordinator Integrity and Ethical Standards

Responsible for all matters that result in official misconduct proceedings.

Information Asset Custodians

a. specify information security classifications under delegation for information and information management requirements. Custodians with delegation 1407 will also grant access to information and only they can authorise disclosure of confidential information,
b. are accountable for the management and protection of information assets/systems. This includes ensuring appropriate system security controls are implemented and all procedures are documented, maintained and followed,
c. conduct 'Threat and Risk' assessments on the relevant information assets/systems. Additional roles and responsibilities for Information Asset Custodians are defined in the Information Management Policy,
d. implement controls in alignment with this policy and associated standards to mitigate cyber risk to tolerable levels as per the Enterprise Risk Management Framework,
e. conduct periodic evaluations of cyber security controls within their area of responsibility and implement improvement plans,
f. notify the Executive Coordinator Cyber Security and Information Solutions or of cyber incidents and breaches in a timely manner,
g. notify the Executive Coordinator Cyber Security and Information Solutions of the outcomes of risk identification and evaluations in a timely manner.

System Administrators

a. develop, implement and monitor security procedures on systems in their charge.
b. monitor the security of their information and systems, and where necessary advise the Information Asset Custodian of security problems.

Security Specialists

Research, develop, recommend, implement, maintain and monitor security systems and procedures on Council systems in consultation with the Business Innovation and Technology Services Branch.

Enterprise Architecture Team

Develop information security architecture**,** approve information security design documentation, assist in planning and transitioning to required information security and ensure alignment to overall business needs and architecture.

All Councillors and employees

a. report an information security incident in accordance with the Information Security Incident Management Standard.
b. use Council's information systems and associated processes in a security conscious manner according to Information Security Policy, Information Security Standards and the Code of Conduct – Standards of Conduct Part 3 (iv) Privacy.

CITY OF GOLDCOAST.

The Information Security Policy is supported by a range of mandatory standards.

For advice on these standards, please contact the Executive Coordinator Cyber Security and Information Solutions.

Information Security Access Management Standard (iSpot #74171314)
How we provide, manage and revoke access.
Applies to Information Asset Custodians, System Administrators, and Security Specialists.

Information Security Classification Standard (iSpot #74164641)
How we assess the value and sensitivity of information and information systems.
Applies all employees, especially Information Asset Custodians, and Councillors.

Information Security Incident Management Standard (iSpot #74163881)
How we categorise, respond and escalate information security incidents.
Applies to all employees and Councillors.

Information Security Risk Management Standard (iSpot #74582096)
Describes what information security risk is and how it is assessed.
Applies to Information Asset Custodians.

Logging and Monitoring Standard (iSpot #74171023)
Describes what is recorded in a system as evidence of activity and actions.
Applies to Information Asset Custodians, System Administrators, and Security Specialists.

Patch Management Standard (iSpot #74164443)
Describes target remediation times for vulnerabilities.
Applies to Information Asset Custodians, Systems Administrators and Security Specialists.

Remote Access Standard (iSpot #74171277)
Ensures the security of connections from untrusted networks.
Applies to all employees and Councillors.

Secure Disposal and Sanitisation Standard (iSpot #74431949)
How we destroy information when no longer required or ensure information can't be recovered or reassembled.
Applies to Information Asset Custodians and roles responsible for information assets.

Supply Chain Security Standard (iSpot #74163162)
Assists with selection of appropriate contracts and builds security into supplier agreements.
Applies to all employees especially Procurement and Council Contract Representatives

Vulnerability Management Standard (iSpot #74170892)
Describes activities and approvals for vulnerability scanning.
Applies to Information Asset Custodians, Systems Administrators and Security Specialists.