INFORMATION SECURITY MANAGEMENT POLICIES

Table of Contents

Information Security Management Policies		
Owner: Head of IT	Area: IT	POL No: 391
Date of Commencement: 25/02/2020	Approval Authority: ET	Date Approved: 25/02/2020
Amendment 0	Date of Next Review: 25/02/2022	Review: 2

INFORMATION SECURITY MANAGEMENT POLICIES

1. Scope

This policy outlines the general principles for managing information risk at City of Parramatta Council. This policy applies to anyone using any form of information technology to process, store and transmit digital information including employees at City of Parramatta Council, contractors, 3rd-party providers and Councilors.

2. Purpose

City of Parramatta Council is committed to building a high quality Information Security Management System (ISMS).

This is achieved by:

(a) Managing access to Council information and customer information based on business need and sensitively of information.

(b) Implementing a set of controls to manage the implementation of security in line with this policy.

(c) Periodically reviewing risks and the effectiveness of controls intended to manage those risks.

3. Definitions

Sensitive Information or Data is information that has been classified as Sensitive, Sensitive (Personal), Sensitive (Health), Sensitive (Law Enforcement), Sensitive (Legal) or Sensitive (NSW Government).

Privileged Account is an account that permits administrative-level changes.

Administrative-Level Changes are modifications to configuration items that modify security controls and settings.

Authorised Individual is a named individual who has been explicitly granted access to a system or resource

Least Privileged is an important concept in computer security, promoting minimal user profile privileges on computers, based on users' job necessities.

Need-to-Know is access control restrictions to information that deny access by default unless access is explicitly allowed as determined and authorised by the information or business owner.

System is Information or Communication Technology equipment storing, transmitting or processing digital information

System Owner is the named Information or Communication Technology, information or business owner.

Privileged Tasks are tasks that requires Administrative-Level privileges to complete.

Inappropriate Access is the denied access to Information or Communication Technology or Information based on policy.

Information is digital data or information

4. Policies

4.4 Access and Account Management Policies

The following principles manage the security of our system accounts and access to those accounts:

(a) User accounts and passwords will be used to manage access

(b) A secure procedure must be defined and maintained for creating, allocating, unlocking and deleting accounts

(c) Privileged accounts must not be used to perform non-privilege level tasks

(d) Privileged accounts must be limited to authorised individuals responsible for administering the system.

(e) Testing and development accounts will not be used in production environments

(f) The security principles of least privilege and need-to-know will be used

(g) Users will be positively identified prior to being granted access to sensitive systems and information

(h) All system owners have responsibility to manage access to their systems

(i) Systems will be logged and monitored for potential inappropriate access

(j) Remote access will be provided by a virtual private network and all users will be positively identified prior to access being granted.

4.5 Information Technology (IT) Asset Management Policies

City of Parramatta Council's IT assets must be managed in the following way:

(a) IT assets with attractive resale potential shall be managed

(b) City of Parramatta Council will maintain an inventory of assets including hardware, software, license and virtual assets.

(c) Assets maintained in an asset management database will have identified owners

(d) Acceptable use of assets will be identified, documented and implemented

(e) Assets will be returned to City of Parramatta Council if employment is terminated

(f) We will maintain an inventory of our license assets and detect risk of being under-licensed (at risk of a compliance audit) or over-licensed (wasting money on unnecessary software purchases).

(g) IT assets will be configured to meet a secure configuration baseline.

4.6 Password Policies

The following principles apply to all accounts storing, processing and transmitting Council information:

(a) Passwords should have a sufficient level of factors, length and complexity to delay an attacker's attempt in systematically checking all possible passwords until the correct one is discovered.

(b) Council should define authentication and password management standards.

(c) Council should review the minimum password length and complexity annually to ensure it remains sufficient to protect system and user accounts.

(d) Council should enforce password management standards on all system and user accounts under its security domain.

(e) Privilege passwords for systems must be stored in a secured location that provides adequate encryption, access-controls, role-based delegation, multi-factor authentication and auditing.

(f) Council should ensure that vendor supplied and/or default passwords are not used on any system.

(g) Council authentication and password management standards must protect remote access, sensitive information and privileged access to critical systems against credential re-use attacks.

4.7 Information Technology Business Continuity & Disaster Recovery Policies

The following principles establish Councils approach toward resilience, availability and continuity of processes, systems and services. It defines requirements around business continuity, disaster recovery and crisis management processes. The overall approach is guided by Risk Management and the Business Impact Analysis (BIA) assessment. Including defined time objectives for Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

(a) Mission critical system, process or Service Owners must ensure proper Business Continuity and/or Disaster Recovery that is in line with the tolerance for disruption in case of disaster.

(b) Continuity plans must include appropriate "last stand" environment, that provides core functionality (at the minimum), and a plan to fail-over to that environment. Considerations for business-as-usual resumption must also be included.

(c) No mission critical system, process or function could be deployed in production without appropriate continuity plan.

(d) Plans must be tested bi-annually with a full test completed every 5 years. Issues identified and addressed.

(e) Maximum time for recovery (RTO) starts from event detection until the core functionality is operational. Services are grouped into Tiers that define maximum RTO and RPO

(f) Following the completion of a BIA assessment, IT will adjust the existing plans to meet any new requirements within 12 months

(g) Lockdown procedure should be activated when disaster is declared.

4.8 Network Communications Security Policies

The following principles manage the security of our communications:

(a) Networks should be segregated based on criticality and risk profile.

(b) Communication should be implicitly denied unless authorised.

(c) Network access should be controlled based on the sensitivity of resources being granted access

(d) Network access is supplied and all users should be familiar with the Acceptable Use Policy

4.9 Cryptography & Encryption

The following principles ensure Council implements appropriate encryption & cryptography to ensure confidentiality of sensitive information. Council deploys cryptographic mechanisms to mitigate the risks involved in storing sensitive information and transmitting it over networks, including those that are publicly accessible (such as the Internet).

City of Parramatta Council will ensure:

(a) Sensitive data is encrypted appropriately when traversing an untrusted network

(b) Sensitive data is encrypted appropriately when stored on an untrusted network

(c) Strength of selected encryption corresponds with information classification

(d) Cryptographic keys will be securely managed

(e) Only approved cryptographic algorithms will be used

(f) Weak or vulnerable cryptographic algorithms will not be used.

4.9.1 Cyber Security & Information Lifecycle Management

Information Security and its lifecycle rely on the information being correctly classified. The Information Security Classification Policy establishes overall requirements on how to handle information. Examples for how to handle different types of information can be found below.

Our values are underpinned by an 'open and transparent government', ensuring the Public has access to official information, however, all employees must consider how to handle internal as well as customer data, as it may be protected by laws and regulation. Employees must also understand how sensitive information, that could cause business impact to Council, must be handled and protected.

All employees share the responsibility for ensuring our information receives an appropriate level of protection by observing this Information Classification policy:

(a) City of Parramatta Council to apply a classification degree of sensitivity and criticality to the information created, collected, and disseminated within the business.

(b) City of Parramatta Council will not transmit or receive sensitive information that has not been appropriately encrypted using end-user technologies such as email, instant messaging, chat, etc.

(c) City of Parramatta Council to place controls relating to the type of information and its need to remain confidential and secure.

(d) Testing and development data will not be used in production environments

(e) Information should be labelled to ensure appropriate handling

(f) Manage all removable media with the same handling guidelines as below

(g) Media being disposed of must be securely deleted after observing the relevant retention period.

(h) Media containing company information should be protected against unauthorised access, misuse or corruption during transport

(i) Critical and security event logs must be protected to ensure the integrity and availability of the captured event logs

(j) Critical and security event logs must be retained for a minimum of 12 months after action is completed. In accordance with the New South Wales Local government records (GA39), the length of retention needs to be determined by Council and will depend on the system, information and the nature of the risks faced.

4.10 Mobile & Bring Your Own Device (BYOD)

This policy intends to be as unobtrusive and as flexible as possible with regard to the Bring Your Own Device (BYOD) usage to maintain City Of Parramatta Council's autonomy whilst ensuring Council has the ability to protect our customer and corporate data.

(a) The primary focus will be on configuration / posture checking and monitoring of compliance of devices, with the least restrictive principles that reasonably achieve the required security objectives, rather than enforcement of restrictions. Where restrictions are applied, they will be selective and based on protecting sensitive information from unauthorised disclosure and dissemination.

(b) BYO devices requesting access to City of Parramatta Council systems will be required to install a Mobile Device Management (MDM) agent to house and encrypt Council data.

4.11 Operational Policies

Technology operational practices at City of Parramatta Council are set through the following principles. City of Parramatta Council procedures not adhering to standard Information Technology Infrastructure Library (ITIL) procedures should be documented for operational activities.

(a) Backups must be taken regularly to meet RPO

(b) Backup restoration process should be tested at least annually

(c) Plans and procedures must be documented, that recover business functions to meet RTO.

(d) All changes should be managed and evaluated by multiple people

(e) Capacity should be evaluated and planned for

(f) We will comply with software licensing requirements and authorise software before it's used

(g) ICT retains the right to remove any piece of software that is deemed unsuitable or unacceptable to the Council.

(h) Software installation should be limited and unnecessary software should be restricted

(i) Logs must be configured and forwarded to the centralised logging platform

(j) Any operational incidents should be managed according to our standard Incident process and defined service levels.

4.12 Personnel Security Policies

The principles of personnel security include:

(a) Security responsibilities will be outlined in job definitions

(b) All employees and users will regularly attend security awareness training

(c) All employees and contractors have a duty to report security incidents or weaknesses

(d) Upon employee termination, access and return of assets will occur in a reasonable time frame

(e) Nametags must protect the anonymity of the employee from public by default.

4.13 Physical & Environmental Security Policies

The principles of physical and environment security include:

(a) City of Parramatta Council will provide secure areas to work

(b) We will secure our IT equipment wherever it may be with security controls proportionally sufficient to protect Council assets based on the asset's level of criticality and/or value to Council.

(c) We will restrict access to our buildings and offices to appropriate personnel.

4.14 Privacy Policies

The principles of privacy include:

(a) Manage controls around collection

(b) Manage controls around access and use

(c) Manage controls around dissemination and destruction

(d) We will comply with the appropriate privacy laws within NSW

(e) We will manage data privacy in accordance with our Privacy Policy

4.15 Incident Management Policies

This policy sets out the general principles and guidelines to ensure that City of Parramatta Council reacts appropriately to any actual or suspected IT incidents. City of Parramatta Council has a responsibility to monitor incidents that occur within the organisation that may breach confidentiality, integrity or availability of information or information systems.

The City of Parramatta Council IT Team will:

(a) Investigate and document major incidents.

(b) Anticipate IT major incidents and prepare response plans accordingly

(c) Contain, eradicate and recover from an incident

(d) We will invest in our people, processes and technologies to ensure we have the capability to detect and analyse an incident when it occurs

(e) In responding to an incident, we will put the protection of customer data as our top priority

(f) Learn from and improve the incident management function.

4.16 Supplier & Third Party Data Management Policies

This policy sets out the general principles and guidelines to select, engage, and oversee vendor access to City of Parramatta Council data.

Agreements with 3rd-party suppliers should include:

(a) Demonstration of compliance: a clause requiring the provider to provide independent evidence that its operations and controls comply with contractual requirements. This could be achieved, for example, by third-party audits that are agreed upon by the provider and Council.

(b) Response time to vulnerabilities: a clause requiring the provider to provide, in a timely manner, proper treatment for known vulnerabilities that may affect the Council's business.

(c) Adherence to security practices: a clause requiring the provider to adhere to the Council's security practices, and to communicate any situations where this adherence is not achievable, helping to prevent security gaps or conflicts that could impair security performance.

(d) Notification about security breaches: a clause requiring the provider to inform the Council in a timely manner, regarding any security breaches that may affect Council's business. Generally, this clause relates to data breach notification laws that affect either the Council or the provider, or both.

(e) Right to audit: a clause ensuring Council has the right to audit and test the security controls periodically, or upon significant changes to the relationship.

4.17 Environment Change Policies

This policy sets out the general principles for the development and implementation of new solutions (applications, software, hardware and services) both internal and customer facing. These include business, IT and security solutions that add, move, delete or changes Council's existing environment

(a) Business, IT and Security requirements will be included and incorporated with all product development

(b) We will complete a security and impact analysis of all changes to the environment to avoid or minimize negative impact of new solutions.

4.18 Threat & Vulnerability Management Policies

This policy sets out the general principles for managing security threats and vulnerabilities both in our environment and in our products.

City of Parramatta Council will ensure:

(a) We will manage security vulnerabilities in our IT products and services, including issuing updates, patches or advisories

(b) We will manage security threats against our IT assets, including internal and hosted environments.

4.19 Audit & Compliance Management Policies

This policy sets out the general principles for managing the audit and compliance program to validate implementation of the City of Parramatta Controls Framework.

City of Parramatta Council will ensure:

(a) We implement technology-focused operations, security and privacy controls to ensure they comply with relevant internal policies, regulations and external industry standards

(b) Audits are coordinated and delivered as appropriate to achieve a high level of confidence in our control environment, as well as to achieve internal or external certification.

(c) City of Parramatta Council seeks external validation of the implementation of our operational, security, privacy and other controls

(d) City of Parramatta Council maintains a consolidated view of all its relevant control objectives, activities and tests (City of Parramatta Council Controls Framework)

(e) City of Parramatta Council maintains a consolidated view of all its relevant control exceptions, accepted risks and compensating controls.

4.20 Data Breach Notification Policies

Reporting data breaches principles include:

(a) Will adhere to the requirements listed under the Privacy Act (1988) to ensure Notifiable Data Breaches (NDB) are reported

(b) We will maintain a Data Breach Policy

(c) We will update our Data Breach Policy when laws and regulations are updated

(d) We will review our Data Breach Policy every 12 months to ensure we meet the requirements of applicable laws and regulations.

5. Associated Documents

REFERENCES	NSW Privacy Laws • https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/ppip-act Data Breach Guidance for NSW Agencies • https://www.ipc.nsw.gov.au/data-breach-guidance-nsw-agencies Fact sheet - NSW Public Sector Agencies and Notifiable Data Breaches • https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-notifiable-data-breaches
POLICIES	• Information Security Classification Policy • Information Technology Acceptable Use Policy
ATTACHMENTS	