INFORMATION, COMMUNICATION TECHNOLOGY SECURITY MANAGEMENT POLICY

Policy Type: Operational Policy **Policy Owner: Manager Information, Communications and Technology**	**Policy No.: OP-035** **Last Review Date: 21/06/2022**

Policy Objectives

Information owned or licensed to the City of Melville (the City), whether held and managed by City staff or by third parties, is an asset that requires protection.

The objectives of this policy is to describe the requirements of information asset protection in terms of:

- Confidentiality - protecting sensitive information from unauthorised disclosure or interception;
- Integrity - safeguarding the accuracy and completeness of information and computer software;
- Availability - ensuring that information and vital services are available to users and not disrupted by security breaches.

The Information, Communication Security Technology Management Policy will lessen the range of Information, Communication and Technology (ICT) threats, thereby reducing the risks to which the City is exposed.

Policy Scope

This policy covers the management of security for the City's information. This includes the technology infrastructure, applications, systems, people and services that store, process and access, the City's data and information.

Information management and security is the responsibility of everyone in or associated with the City. This policy applies to all staff, volunteers, contractors' and consultants working for the City, using the City's resources or accessing the City's technology environment or information.

Public Access workstations and WIFI are excluded from this policy.

As an Operational Policy, Elected Members are excluded from specific accountability. They are expected to access, use and care for equipment and information in alignment with the Code of Conduct for Elected Members, Committee Members and Candidates and any concerns raised with the Manager ICT Services in the first instance.

Policy Statement

The City has nominated the Manager Information, Communications and Technology to have responsibility for the City's compliance with the:

- State Records Act 2000 (WA);
- Freedom of Information Act 1992;
- Electronic Transactions Act 2011;

And general adherence to other relevant legislation including:

- Privacy Act 1988 (Commonwealth)
- General Data Protection Regulation (GDPR) – an Act of the European Parliament with extra-territorial reach

The Manager Information, Communications and Technology is accountable for use of the City's resources and to ensure the requirements for information security are satisfied in accordance with the principles of risk management, including:

- protecting the availability, confidentiality and integrity of information.
- control of access to and proper use of information and information systems.
- authentication of users; and
- non-repudiation of electronic transactions, data and information.

The City's approach will be based on relevant international standards for information security management. This policy is structured to align with the National Institute of Standards (NIST) Cyber Security Framework.

1. Identify

Information Security Risk and Compliance

- ICT Services has responsibility for co-ordinating the ICT Security Management Policy and its related Systems Procedure. ICT Services employees are empowered with sufficient and appropriate authority to be capable of establishing and maintaining the effectiveness of the City's IT Security procedures.
- The City of Melville ICT Security System Procedure will articulate the standards, controls and procedures that exist to manage information security.
- A specific risk register for identified technology and information risks will be maintained by Risk Services.
- The level of compliance with any applicable standards is to be reported to the Information Governance and Steering Oversight Group (IGSOG) and the Financial Management, Audit, Risk and Compliance Committee (FMARCC) .

Vulnerability Management

- Security patching and vulnerability management processes will be maintained by ICT Services. Patching will occur based on risk assessment using the Australian Government Essential Eight recommendations as a basis.
- The City will formally review and assess vulnerabilities in accordance with the City's approved Cyber Security Testing and Assessment Plan.

Asset Management

- All City owned technology hardware will be assigned an asset owner. The asset owner is responsible for the assets physical security and ensuring usage is in accordance with legislation, policies and procedures.
- All software applications used for City activities will be identified and an application owner specified. This position is responsible for ensuring use of the application complies with licensing requirements and users comply with relevant legislation, policies and procedures as applicable;
- All information held by the City will be assigned an owner. The information owner will be responsible for ensuring appropriate information protection standards are applied in accordance with the assessed data classification.

Systems Acquisition

- All systems or software acquisitions will be in accordance with the City's "New Software Application" procedure. This procedure is applicable for all software regardless of cost or type.
- Approval to utilise any application that accesses, manipulates or stores City information will be at the discretion of the Manager ICT or delegate.
- All software acquisitions will be required to meet appropriate legislation, policy and risk requirements.

Bring Your Own (BYO) Hardware

- The City supports BYO capability subject to meeting appropriate access and security requirements
- No BYO hardware will be allowed to be directly connected to the City's core (in office) network.
- Virtual Private Network (VPN) access will not be allowed for non-City equipment.

Third Party Risk Management

- Access to the City's information by contractors or consultants will be in accordance with all other aspects of this policy.
- Real time access to the City's environment by contractors and consultants may be time or location controlled and will be logged

Protect

Third Party Risk Management

- The City's procurement contracts will include appropriate clauses to ensure information supplied to contractors or consultants are used for prescribed purposes only

Backup

- Information held by the City will be backed up on a regular basis to industry standards, protected from unauthorised access or modification and available in a timely manner when required;
- Backup architecture can be found in the Data Backup and Recovery Directorate Procedure.

Information Security

- All information will be classified according to a standard security level of private, secure or unclassified.
- All information classified as private or secure will be limited in access in accordance with "need to know" principles.

User Access Management

- All user access related requests including new users, contract extensions and altered access requirements will be logged and approved in accordance with relevant approval processes.
- All user terminations will be in accordance with supplied termination or contract end dates.

Software as a Service (SAAS) Security

- Use of SAAS application is considered an application acquisition. The same requirements and assessments will apply.
- All SAAS delivered applications are required to meet at least the minimum standards of security as prescribed by the City.
- All SAAS delivered applications will be assessed for risk to the City information;

Change Management

- All application changes including configuration modifications but excluding single user modifications, will be completed in accordance with the City's Technology Change Management Processes. The change must be authorised by the City Technology Change Management Approval Group before commencement.
- The change request must include a risk assessment to ensure information security and operations are not compromised and incorporate mitigation controls where applicable.

Physical Security

- The City will utilise data centre facilities that meet or exceed Tier Three Data Centre rating for all production service delivery.
- Access to the City's Disaster Recovery server room shall be limited to designated Technology team members only and access controlled by electronic door controls.
- Network Cabinets used throughout City premises will be locked with access by City authorised personnel only. All equipment located in the cabinets will be authorised by ICT Services.
- Where equipment is portable or exposed to public access, additional security controls may be mandated to protect against physical and information loss or damage.

End User Protection

- ICT Services will supply and maintain appropriate security mechanisms on all City owned devices.
- Access to the City's applications and information will only be through protocols and methods approved and maintained by ICT Services.

Network Security

- ICT Services will implement and manage appropriate security controls across networks that the City owns or utilises to ensure security of the City's information;

Human Resources Security

- The City will implement appropriate employment vetting and security clearance processes before and during employment where access to private or sensitive information is required;
- Each consultant, contractor or volunteer managed by the City who will have access to sensitive, private or copyright information shall sign a Confidentiality/Non-Disclosure Agreement.

Detect

Information Exchange

- The City will monitor security breaches and imminent threats, and exchange information with peers or other relevant authorities where appropriate.

Logging and Monitoring

- ICT Services will monitor equipment logs which will be analysed regularly in order to identify potential security or privacy issues and risks. Anomalies will be addressed as an urgent priority.
- User access and changes will be formally logged, authorised and held as a record of activity.

Respond

Investigations of security incidents will be conducted on an as required basis and reported to the IGSOG for improvement actions.

Any known privacy breaches will be managed in accordance with mandatory notification principles.

Breaches of ICT Security will be dealt with in accordance with established breach of contract or employment procedures.

The City will develop and maintain a Security Incident Management Plan.

Other References that may be applicable to this Policy

Legislative Requirements:	Local Government Act 1995
	State Records Act 2000
	Freedom of Information Act 1992
	Data Protection Act 1998
	Surveillance Devices Act 1998
	Local Government (Administration) Regulations 1996
Delegated Authority:	N/A
Plan / Policy / Framework:	Knowledge and Information Management Framework
	Record Keeping Plan
Procedure:	ICT Security Systems Procedure
Work Instructions / Process Maps:	N/A
Forms / Supporting Documents (internal):	
Supporting Documents (external):	PCI DSS V3.2
	NIST Cyber Security Framework V1.1
	ISO27001

Origin/Authority

EMT	02/11/2011

Reviews

Manager Information, Communications & Technology	21/06/2022
Manager Information, Communications & Technology	08/05/2017
Manager Information, Communications & Technology	16/11/2014
Manager Information, Communications & Technology	18/09/2014