IT Systems Security Policy

Purpose

To protect the City of Sydney's (City) Information Technology (IT) resources and systems.

The policy describes the key principles and compliance requirements to safeguard the City's IT resources and systems from:

- unintentional misuse and mismanagement by authorised users
- intentional acts, such as theft, sabotage, manipulation, and misuse of the City's IT resources by internal and external, authorised and unauthorised users.

This policy should be read in conjunction with the City's Code of Conduct and the other policies and related procedures referred to in this document.

Scope

This policy applies to all persons using City IT resources, including Councillors, staff, contractors, volunteers and third parties who have been authorised to access some of the City's information systems.

The following IT resources are within scope of this policy:

- all physical assets that process and store information that are owned and/or operated by the City
- all software authorised for use by the City to conduct its business, including those provided by cloud providers.

The provisions of this policy apply to the City's IT resources irrespective of the location of the asset.

Definitions

Term	Meaning
Authentication	The process of determining whether someone or something is who or what it claims to be, usually through the process of password logon.
Authorisation	The granting of rights to access part or all of an information system, based on job role and responsibilities.
Authorised user	An "authorised user" is an employee, a contractor, a Councillor, a volunteer or a representative of a third-party who has been granted access to some of the City's IT resources.
Remote Access	The ability to access City information systems and network from outside the City's network perimeter.

Term	Meaning
Removable Storage Media	A device for storing data that can be removed from a computer whilst the system is running. Examples include CDs, DVDs, and USB drives.
User	A person authorised to access City information systems.
Unauthorised Use	When a person does not have permission to access a system, equipment, device, network or information.

Secure use of IT systems and services

Prohibitions

- Access to products, features and services will be blocked or denied where those items introduce a risk to the integrity or security of the City's IT systems and services.
- The City's IT systems must not be used to create, distribute, access or store information or data that is detrimental to the integrity and security of City IT systems and services.
- Users must not attempt to circumvent the security mechanisms at either City of Sydney or other Internet sites. The possession and use of tools for hacking information systems' security are prohibited.
- Users must not use their City of Sydney email address for personal website registrations, i.e. for username and/or password combinations.

Clear Screen Requirements

- Computers should be locked when unattended and protected by screensaver passwords.
- Screensaver will be enabled on computers after fifteen minutes of idle time.

City-Issued Mobile Computing Devices

- All computing devices and equipment issued to individuals by the City remain the City's property and as such they are also subject to this policy.
- Mobile computing devices and equipment must never be left unattended in public places.
- Mobile computing devices and equipment must be stored in a locked location when unattended.
- Laptops and other portable devices must be carried as hand luggage when travelling.

Introduction of New IT Systems, Software, and Devices

- Technology & Digital Services (TDS) is responsible for ensuring the City's IT systems, services and infrastructure are designed, developed, implemented and maintained to meet appropriate security standards.
- To preserve the City's standards, the following actions are prohibited:
    - installing or using software not previously authorised by TDS for use on City computers
    - connecting any device, other than a USB drive to City's network that has not been authorised by TDS
    - downloading programs or executables from the Internet or emails.

Authorised Access

Access to the City's IT systems is restricted to authorised users only. An authorised user could be:

- an employee of City of Sydney
- a contractor of City of Sydney
- a Councillor
- a volunteer, or
- a representative of a third party (company, partner, association etc.) who has been authorised to have access to some of the City's IT systems.

Each user will be issued with a unique User ID and password to provide accountability of actions of unauthorised modification, destruction and disclosure of information, whether intentional or inadvertent.

Once a unique User ID is assigned to an individual, it will always be associated with that person. The same User ID must not be reassigned to another person or entity under any circumstances.

A user may have no more than one User ID, unless the Business Unit Manager and Cyber Security Manager have authorised the allocation of an additional account.

A user must be authenticated each time they attempt to log onto the City's network or systems to protect the City resources from unauthorised use.

Each user's level of access is determined by business requirements. Users will be granted the minimum level of access necessary to perform their duties. If the business requirements or user's duties change, then the user's level of access must be revised accordingly.

The use of shared, guest and other such generic user accounts is not generally permitted. Any exception requires the approval of the Chief Technology & Digital Services.

Where requirements dictate that a real user account should not be used then a Service Account or Resource Account is permitted. Ownership of Service and Resource Accounts will be assigned to an appropriate individual who is responsible for ensuring all usage is legitimate.

Access to IT systems and resources must be disabled as soon as possible upon termination of employment.

Refer to *the IT Network Access Control Standard* and the *TDS Access Control Procedure* for implementation of these policy statements.

Password Security

Unique initial passwords must be provided to the user through a secure and confidential process. Initial password must be changed upon first logon.

Authorised users are responsible for the security of their passwords and accounts. Users must keep passwords secure and not known to others. Authorised users must not allow others to use their account.

New systems must meet the minimum password requirements as described in the *Password Management Standard*.

Refer to the *Password Management Standard* for implementation of these policy statements.

Remote Access

Remote Access may be provided to authorised users who need to access the City's information systems from outside the City's network perimeter. Remote access is provided for official

business purposes only and must be approved by the Business Unit Manager and Cyber Security and Risk Manager.

Remote access to the City's information systems from outside the City's network perimeter must require registration and use of two factor authentication (2FA).

Refer to *TDS Access Control Procedure* for implementation of these policy statements.

Responsibilities

All users of the City's IT systems and services have IT Security responsibilities. Some roles have additional responsibilities which are outlined below.

All Users must:

- undertake mandatory cyber security training modules on induction and as required periodically or when requested by management
- ensure the security of their account and password as defined in the Password Management Standard
- operate and use IT resources in accordance with the supplementary procedures listed in the References section of this document
- ensure the care and secure storage of IT devices and equipment assigned to them
- report the loss of City-issued equipment or devices immediately
- report information security incidents, breaches and weaknesses to their manager, supervisor or the IT Service Desk in a timely manner.

Business Unit Managers will:

- ensure that new employees read and understand this policy during their induction to the City and understand their IT security responsibilities
- update existing staff about the City's requirements for IT security
- advise the relevant system administrators of any access changes that are required as a result of employee terminations, transfers or role changes
- recover all access cards, keys and tokens from terminated employees (including contract employees) and return these to the issuing unit
- ensure that security incidents, breaches, and weakness of which they are notified are appropriately escalated.

Business System Owners will:

- ensure operational management of a business system, in terms of its maintenance, utility, reliability and planning for any further upgrade or development work is undertaken
- implement strategic objectives of their information system to ensure it meets the business needs of the City and is appropriately available, secure and sustainable
- ensure overall management and control of their system, and compliance with all relevant legislation and City policies is maintained
- approve requests for access to their business systems
- establish and conduct periodic audits of access to the system to ensure only users with a legitimate business need have access to their system. The completion and outcome of such audits must be recorded and reported to the Cyber Security and Risk Manager.

Chief, Technology & Digital Services will:

- establish a Technology & Digital Services framework of policies, procedures, controls and audit
- ensure the physical and environmental security of key information technology assets, including, but not limited to, servers, cabling, communications devices, consoles, databases, backup media, etc. is safeguarded
- report on:
  - security incidents, threats and malfunctions that may have an impact on the City's information technology systems
  - compliance with policies, standards and procedures
- review and manage significant information security incidents and investigations
- make recommendations for appropriate policies, procedures or controls to ensure the security of new or existing systems
- review any requested exceptions to the City's security policies and approve/reject the request, delegating or escalating, as appropriate.

Executive Director, People Performance & Technology will:

- ensure the CEO and Business System Owners are informed of any significant information security issues and the status of the City's IT security
- promote IT security to the City's senior management

  ensure IT security policies and standards are developed, implemented, and periodically reviewed.

Policy compliance

Breaches of this policy will be investigated by an appropriate person appointed by the Director, People Performance & Technology. Disciplinary action may apply. This may include termination of employment for serious misconduct or other action in accordance with the City's Disciplinary Procedures.

Where a suspected breach may be an offence under State or Federal law, the City will refer this to the appropriate law enforcement agency.

Consultation

The following areas were consulted in the drafting of this policy:

- Technology & Digital Services
- Legal & Governance.

References

Laws and Standards
• ISO 27001 Information Security Standards • IT Security Standard • Password Management Standard • IT Network Access Control Standard
Policies and Procedures
• Code of Conduct • Internet Policy • Email Policy • Social Media Policy • Mobile Device Policy • Records Management Policy • IT Asset Acquisition and Management Policy • TDS Access Control Procedure • Access to Information Policy

Review period

This policy will be reviewed every 2 years.

Approval Status

The Chief Executive Officer approved this policy on 26/2/25

Monica Barone PSM, Chief Executive Officer

Approval History

Stage	Date	Comment	TRIM Reference
Original Policy	12 February 2013	Endorsed by the Executive	2013/023125
Reviewed	8 March 2016	Endorsed by the Executive	2016/180614
Reviewed	1 August 2018	Fit for purpose. No change. Endorsed by the Executive	2018/433275
Reviewed	16 October 2020	Minor amendments including updating access, remote access and recording/reporting audits.	2018/433275

Stage	Date	Comment	TRIM Reference
Reviewed	12 October 2022		2018/433275
Reviewed	26 February 2025	Removal of prohibition to connect the City's device to third-party corporate networks as obsolete. Addition of two new requirements: 1 Recommendation of not to use City of Sydney email addresses for personal website registrations, and 2. Complete mandatory security training on induction or as required.	2018/433275
Commence Review Date	26 May 2026		
Approval Due Date	26 February 2027		

Ownership and approval

Responsibility	Role
Author	Cyber Security & Risk Manager
Owner	Chief Technology & Digital Services Officer
Endorser	City of Sydney Executive
Approver	Chief Executive Officer