CITE Managed Services

ICT Security Policies and Procedures

Contents

ICT Security Policies and Procedures

General staff responsibilities

When using CITEMS ICT facilities, all staff have the following responsibilities:

- Staff are personally responsible for their use of ICT systems
- Comply with all regulatory and organisational requirements
- Seek advice when unsure if the actions breach ICT Security Policy
- Take steps to ensure that any systems under their control are reasonably protected from theft, damage, loss or unauthorized access
- Log out of the system when leaving the workstation
- Secure own password and not use other staff member's credential to access the company's systems
- Staff are personal responsible for any breach logged against their user account
- Immediately report any security incidents or breaches

Breaches and consequences

Appropriate action will be taken when:

- There is an external or internal complaint or a report against an employee's use of the ICT systems
- An issue is identified through routine monitoring or auditing activities
- System use causes performance issues due to heavy or inappropriate usage
- A breach of policy is suspected

ICT Systems Security

Physical Access

Physical access to ICT systems must be restricted to authorized personnel only.

Additional requirements are listed next.

Workstations

- Workstations must be kept clear of any visible items containing any sensitive or confidential information (e.g. passwords, company's documentation, client's data etc.)
- Portable devices must be secured to the desk with a tether or stored in a locked cabinet
- Ensure computers are locked or shut down if not in use
- When using ICT systems for internal communication or activities, ensure computer screens are not visible to public
- Sensitive or confidential information must be stored only on the systems approved by CITEMS (such as SharePoint or employee's OneDrive)

Password Standards

Policy	Requirements
Password history	Last 10 passwords
Maximum password age	180 days
Minimum password age	7 days
Minimum password length	14 characters
Password complexity enabled	Yes
Account lockout duration	Until unlocked by administrator
Account lockout threshold	5 invalid attempts
Reset account counter after	30 minutes

- Password complexity requirements:
  - Uppercase characters (A-Z)
  - Lowercase characters (a-z)
  - Digits (0-9)
  - Special characters (e.g. !, $, # or %)
- Use 2-Factor Authentication(2FA) or Multi-Factor Authentication(MFA) where it is available;
- Use Password Manager to help remember and store the user credentials securely

Data Sanitization and Disposal

To prevent potential breaches of data, any devices or media used to store sensitive or confidential data must be properly sanitized or destroyed prior to disposal.
(e.g. shred hard copies, use approved sanitization software)

Software updates and anti-malware

All CITEMS ICT systems or systems used to conduct work must:

- **Windows updates:**
    - Have automatic updates configured to check for any updates and download them every 24 hours;
    - Downloaded updates to be installed automatically;
- **Anti-Malware**
    - Have an approved Anti-Malware software installed and configured with Active Virus Detection;
    - Anti-Malware software must be configured to check for and download the updates automatically;

Access Control

User Account Creation

- User accounts for staff members are created once all employment documentation has been signed and approved;

User Account Deactivation

- Staff accounts are terminated in the following cases:
    - Termination of employment.
    - Retirement.
    - Resignation.
    - Violation of the ICT Security Policies and Procedures.

User Account Reactivation

- If account has been incorrectly deactivated, it may be reinstated once the employment details have been verified;

User Account Security

- Account details must be kept secure and never shared with a third party or other employees;
- This applies to any other credentials used by employees to access the CITEMS systems or to carry out work related activities via external applications such as Slack, Cisco WebEx etc.

Other general ICT policies and procedures

Hardware system requirements

All hardware equipment used and deployed by CITEMS must comply with the guideline listed in this policy.

DESKTOP COMPUTER SYSTEMS

- All standard desktop computer systems built by or used at CITE MS must run Windows 10;
- Hardware and software used to build the computer systems must be purchased from the authorised vendors and suppliers in line with the Purchasing Policy;
- Minimum capacity for a desktop computer must be:
    - CPU: 2.4 GHz or higher | RAM: 8GB or higher | USB Ports: Minimum 4xUSB2.0 and 2xUSB3.0 ports

PORTABLE COMPUTER SYSTEMS

- All portable computer systems purchased for use or for provision of service by CITE MS must run Windows OS;
- Portable computer systems must be Dell, HP, Acer, Asus, Toshiba or Lenovo;
- Hardware and software used to build the computer systems must be purchased from the authorised vendors and suppliers in line with the Purchasing Policy;
- Minimum capacity for a portable system must be:
    - CPU: 2.4 GHz or higher | RAM: 8GB or higher | USB Ports: Minimum 2xUSB2.0 or USB3.0 ports
    - Microphone: Yes
    - Web Camera: Yes
    - Speakers: Yes
    - Built-in wireless adapter: Yes (Dual band)

SERVER SYSTEMS

- All server systems purchased for use by CITE MS are to be approved by the ICT Manager;
- Hardware and software used to build the computer systems must be purchased from the authorised vendors and suppliers in line with the Purchasing Policy;
- All server systems are to be supplied with a minimum of:
    - 60 Months warranty
    - 24/7 support

VIRTUAL MACHINES

All Virtual Machines used by CITEMS must follow the minimum requirements set by CITEMS:

- CPU: Number of processors 1; Number of cores per processor 2
- RAM: 4GB
- Storage: 20GB

OTHER ITEMS

- Any other computer devices including computer peripherals and networking equipment are to be purchased from the authorised vendors and suppliers:
    - Microsoft
    - Dell
    - Cisco
    - PLE
    - PC Case Gear
    - Austin Computers
    - Storm computers
    - CDM Australia
    - Fortinet
    - DrayTek
    - Ubiquity
    - Netplus

- All additional computer devices are to be compatible with the other hardware and software used by the CITE MS;
- Any adjustments to these requirements must be authorised by the ICT Manager;
- All hardware is to be supplied with a minimum 12 Months warranty;

POWER SETTINGS

- Set computers to enter sleep mode after 15 to 60 minutes of inactivity;
- Set monitors to enter sleep mode after 5 to 20 minutes of inactivity;
- Disable the screensavers;
- Set monitor brightness to 50% and enable Night Light option;
- Shut Down PCs after use;

Any adjustments to these requirements must be authorised by the ICT Manager.

All hardware is to be supplied with a minimum 12 Months warranty.

Clear desk policy

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is always secure (especially at the end of the day and when they are expected to be gone for an extended period);
2. Computer workstations must be locked when workspace is unoccupied;
3. Computer workstations must be shut completely down at the end of the workday;
4. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday;
5. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended;
6. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk;
7. Laptops must be either locked with a locking cable or locked away in a drawer;
8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location;
9. Printouts containing Restricted or Sensitive information should be immediately removed from the printer;
10. Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins;
11. Whiteboards containing Restricted and/or Sensitive information should be erased;
12. Lock away portable computing devices such as laptops and tablets;
13. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

System Information Record

Information about deployed servers and client computers must be registered using the form below.

SYSTEM INFORMATION

Asset ID	(e.g.0000001)
System Specifications	(CPU, RAM, Storage)
System Description	(Where it is located and who is using it)
Connected Peripherals	(Type and Serial Numbers)

SYSTEM SOFTWARE

Type	**Software Name and Software License/Product Key**
(OS, productivity, anti-virus, etc.)	

SYSTEM CONFIGURATION

Hostname	
IP Address	IP Address: Subnet Mask: Default Gateway: DNS Server/s:
MAC Address	
Mapped Drives	

USER ACCOUNTS

Type	**User Account Name**	**Member of**
(e.g. Admin, Standard, Domain etc.)		(What Group/OU the user belongs to)

Policy Governance

This policy has been developed in line with the following regulatory and organisational requirements:

Regulatory requirements:

- Privacy Act 1988
    - Australian Privacy Principles
- AS/NZ/ISO IEC 27001 Information Technology – security techniques – information security management

Organisational requirements:

- Staff Code of Conduct