

DEPARTMENT OF EDUCATION AND EARLY CHILDHOOD DEVELOPMENT

Information & Communication Technology SECURITY POLICY

The complete policy, supporting procedures and best practice papers
may be viewed at:

www.eduweb.vic.gov.au/intranet/policies/ictsecurity/default.htm



Department of Education and
Early Childhood Development

INTRODUCTION

Information & Communications Technology (ICT) Security Policy awareness and compliance shall increase levels of:

- confidentiality: protecting sensitive information from unauthorised disclosure or intelligible interception
- integrity: safeguarding the accuracy and completeness of information and computer software
- availability: ensuring that information and vital services are available to users when required.

Loss of confidentiality, integrity and availability of information can occur for a number of reasons:

- hardware failure, such a failure of the computer, its storage devices, or the network
- software errors ranging from programming errors in internally developed or third-party packages, or something as simple as a typo in a spreadsheet formula
- accidents, errors, or omissions by anyone using computers, or the information they process
- intentional acts, such as fraud, theft, sabotage, and misuse of information by employees, suppliers, or curious or malicious hackers
- environmental hazards, such as fire, storm or dust.

The ICT Security Policies, if thoroughly implemented, will minimise the range of ICT threats and reduce the risks to which the Department is exposed.

RESPONSIBILITIES

All people who use Information Communication Technology (ICT) in the Department of Education and Early Childhood Development (DEECD) shall:

- be accountable for all use of DEECD systems performed using their user-ID
- immediately inform their manager on becoming aware of any loss, compromise, or possible compromise of information, or any other incident which has ICT security implications.

POLICIES

The highlighted sections are applicable to all people using DEECD ICT services or equipment.

Information Security

Information Security policy: Management shall set a clear direction and demonstrate their support for and commitment to information security through the issue of an information security policy across the organisation.

Information security infrastructure: A management framework shall be established to initiate and control the implementation of information security within the organisation.
Information Assets Classification and Control

Information Assets Classification and Control

Accountability for information assets: All major information assets shall be accounted for and have a nominated owner.

Information asset classification: Security classifications shall be used to indicate the need and priorities for security protection.

POLICIES *continued*

Personnel Security

Security in job definition and resourcing: Security shall be addressed at the recruitment stage, included in employment conditions and contracts, and monitored during an individual's employment.

ICT Security awareness and education: Users shall be trained in security procedures and the correct use of ICT facilities.

Physical and Environmental Security

Secure areas: ICT facilities supporting critical or sensitive business activities shall be housed in secure areas to protect from physical intrusion, theft, fire, flood and other hazards.

Fixed & Portable ICT equipment security: Desktop & portable ICT equipment shall be physically protected from security threats and environmental hazards.

- Before portable ICT equipment is issued to a user, the user has the Manager's approval and is made aware of the security requirements.
- Portable ICT hardware should always be stored and carried in a purpose designed carrying case.
- Users shall exercise reasonable caution to ensure the equipment is not left unattended in public places.

ICT removable media security: ICT removable media shall be controlled and physically protected.

- Removable media should be stored in dustproof boxes and not left on desks, or similarly exposed.
- Appropriate operating procedures shall be established to protect computer media (tapes, disks, CDs), input/output data and system documentation from damage, theft and unauthorised access.

Disposal: A risk assessment shall be performed prior to the disposal of hardware, software and storage media in order to determine the method by which data should be removed.

Access Controls

Business requirement for system access: Access control standards for information systems shall be defined by the system owner on the basis of business needs.

User access management: Formal procedures shall be established to control allocation of access rights to ICT services.

User responsibilities: All users have a responsibility to prevent unauthorised user access:

- Users should keep passwords secret.
- If a password needs to be divulged, it should be changed as soon as possible.
- Users are accountable for all use of DEECD systems performed using their user-ID.
- Users shall not use another person's user-ID and password.
- Passwords shall be periodically changed (as defined in Best Practice-Password Management).

POLICIES *continued*

Network access control: Access to the resources on the network must be strictly controlled to prevent unauthorised access:

- Any access of the internal DEECD networks shall be regulated by dedicated services enforcing security.
- Any user outside the internal DEECD networks shall not be permitted to connect directly to any resource located on the internal network. Access shall be via a managed firewall or a dedicated service enforcing security.
- Desktop computers connected to the Local Area Network (LAN) shall not be connected to the public switched telephone network (PSTN) via modem and phone line.
- In the DEECD facility, Wireless Access Points shall be installed with the LAN Administrator's (ITD) approval and in accordance with Best Practices. In schools, Wireless Access Points shall be installed ONLY on the Curriculum LAN and in accordance with Best Practices.

Access control enforced by operating systems: Access to a computer shall be controlled by the computer's operating system.

Application access control: Logical access controls shall be used to prevent unauthorised access to application systems and data.

Mobile Computing and teleworking

- Personal computers should not be used at home for business activities if virus and operating system update controls are not in place.
- When travelling, equipment (and media) should not be left unattended in public places. Portable computers should be carried as hand luggage when travelling.
- Portable computers shall be provided with an appropriate form of access protection (e.g. passwords or encryption) to prevent unauthorised access to their contents.
- Passwords or other access tokens for access to the Department systems must never be stored on mobile devices where they may be stolen and give the thief unauthorised access to information assets.
- Department computers (including desktops, notebooks and PDAs) shall not be connected to open, unencrypted wireless networks at home or in public places.
- Ad-hoc wireless networks shall not be used.
- Personnel who share their working space (e.g. family members) should not regard or use their ICT equipment as a general purpose computer or network. The equipment contains information assets belonging to the Department and is likely to give privileged access to further assets or use their ICT equipment as a general purpose computer or network.

Communications and Operations Management

Operating procedures and responsibilities must be documented.

- System documentation is a requirement for all the Department's information systems
- System documentation shall be kept up-to-date and available
- Responsibilities of Systems Administrators shall be clearly documented.

POLICIES *continued*

Third party service delivery management

Where service is delivered by a third party,

- Review meetings shall be conducted on a regular basis during the life of the contract
- Rules of engagement shall be included in contracts, clearly establishing roles and responsibilities
- Regular reviews are integral to monthly performance reports. Third party service providers are required to submit regular performance reports to the Contract Manager
- All contract variations shall be written and formally agreed

Network Security management

- Networks shall be managed and controlled.
- All sites shall have a high level diagram showing all connections into the network and a logical network diagram showing all network devices.
- Service Level contracts should include desired security features.

Exchange of Information

- Information classified as confidential or secret shall be encrypted.
- ICT Systems that transfer data to external parties shall undergo a Privacy Impact Assessment (PIA).
- Private encryption keys shall be physically exchanged rather than transferred electronically.
- Privileged access to email servers shall be restricted to administrators
- Email accessed via a web browser shall be encrypted with Secure Sockets Layer and Transport Layer Security (SSL / TLS). Only trusted sources shall be involved in data transfer between business systems.. Trusted sources are personnel or systems formally identified as capable of reliably producing information.
- Data containing private or financial data shall not be left “parked” on hard drives in an unencrypted form during transfer or batch uploads.
- System access and use shall be monitored to ensure conformity to access policy and standards.
- Audit logs shall be detailed in system documentation and shall be designed before a system goes into production
- Business rules shall be established for each system on where the logs are kept, who had access to them and for how long they are preserved
- Audit logs must not be altered
- Repairs and maintenance of systems containing classified data shall be carried out on-site by appropriately cleared, qualified and briefed personnel.
- DEECD shall provide anti-virus software for all servers, workstations and notebooks.
- Network administrators shall run anti-virus scans on all network file servers on a regular basis.
- Network/EduMail administrators shall be responsible for the prompt removal of the virus and investigation of its origin.
- All workstations and notebooks shall run DEECD approved anti-virus software.
- Anti-virus software shall be kept up to date, with virus definitions being updated at least weekly.

Business Continuity Planning

Business Continuity and Disaster Recovery Plans shall be available to protect critical business processes from the effects of major failures or disasters.

Processing, Transferring and Storing Data

Managing data storage: Day-to-day data storage must ensure that current data is readily available to authorised users and that archives are both created and accessible in case of need.

Managing databases: The integrity and stability of the Department's databases must be maintained at all times.

Managing confidential data: Additional measures shall be taken to protect data designated as confidential.

Saving data by individual users: All users of information systems must save their work on the system regularly in accordance with Best Practices:

- Data should not be saved to a local hard disk (C: or D: drive).
- When information and data is stored on local disks (e.g. Notebook computers), they must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

Transferring/exchanging sensitive or confidential data: Sensitive or confidential data/ information shall only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be assured.

Data retention: Data created and stored by the Department's information systems must be retained for a minimum period that meets both legal and business requirements and complies with the *Public Records Act 1973* (addition of the Act).

Systems Maintenance

System maintenance schedules shall be formally planned, authorised and documented. Changes to routine systems operations shall be fully tested and approved before being implemented.

Security Incident Management

- Any person who becomes aware of any loss, compromise, or possible compromise of information, or any other incident which has ICT security implications, shall immediately inform their manager, who shall advise the Call Centre or Manager, Risk Management.
- The relevant line Manager shall ensure that the violation is investigated.
- All security incidents shall be recorded to ensure that details of the incident, investigation, resolution and outcome are documented.
- All observed or suspected security weaknesses in ICT systems and services shall be reported to the Department's Service Desk.

Intellectual property rights (IPR) - ICT equipment must not be used for processing or copying information that in any way breaches or infringes copyright, patents or any other intellectual property rights.

Managing confidential data - Confidential information shall only be processed by authorised personnel. Testing should not be performed on copies of 'live' (production) files that contain sensitive data. When records in any format are no longer active they should be disposed of (either stored or destroyed), according to PROV standards and ARMU guidelines. They should not be held indefinitely in the standard environment.

Compliance

Security reviews of ICT systems: The security of ICT systems shall be regularly reviewed.

Security requirements of systems security incident management: A formal procedure shall be established to deal with incidents affecting ICT security:

- Any person who becomes aware of any loss, compromise, or possible compromise of information, or any other incident which has ICT security implications, shall immediately inform their manager, who shall advise the Call Centre or Manager, Risk Management.
- The Manager, Risk Management shall initiate immediate action to prevent further compromise or loss.
- The relevant line Manager shall ensure that the violation is investigated.
- The General Manager, ITD and Manager, Risk Management, shall assist in the investigation as required.
- The Manager, Risk Management, shall report on the incident to the General Manager, ITD after the investigation is complete, recommending remediation and steps to prevent further breaches.
- All security incidents shall be recorded to ensure that details of the incident, investigation, resolution and outcome are documented.

Internal disciplinary processes: A formal disciplinary process shall be established for dealing with personnel who commit a security breach:

- The course of disciplinary action to be undertaken must be determined by the Secretary (or delegate) on a case-by-case basis.
- The Code of Conduct for the Victorian Public Sector 1995 defines the behaviour expected of employees when utilising information and action that may be taken in the event of breaches.
- There shall be adequate evidence to support an action against a person. Whenever this action is an internal disciplinary matter, the evidence necessary will be described by internal procedures.

External disciplinary processes – reporting to police: Independent of whether the security violation is an internal or external matter, where it is considered a criminal offence, the Police (Federal and/or State) shall be informed.

Compliance with Security policies and standards

Management shall ensure that their area of responsibility complies with the Department's security policies and standards.