ICT Services

DECD Policy – ICT Security

Policy

DECD information is an important business asset and must therefore be protected to preserve its:

- confidentiality;
- integrity;
- availability.

DECD is committed to ensuring its information is appropriately managed according to the South Australian Government's mandated Information Security Management Framework. This will be achieved through the establishment and implementation of suitable controls including policies, standards and procedures.

DECD is also committed to protecting and managing all assets that contribute to the security of DECD information. These assets include physical and environmental facilities, ICT equipment, communications facilities and applications software and packages.

Policy Guidelines

1. ICT Logical Security

Access to information and business processes must be controlled on the basis of business and security requirements, and is subject to the DECD Information Management Policy – Privacy and Confidentiality. Adequate security must be provided to ensure both the protection and the maintenance of system integrity over the information systems, information and documentation at all times.

1.1 Information Asset Classification

DECD information and information assets must be classified to indicate their importance in terms of the three security objectives of confidentiality, integrity and availability. All information assets must have a nominated owner.

1.2 Access Control and Management

Users must only be supplied with the level of access required to perform their work duties. Users must not attempt to gain access beyond their given access privileges.

An effective access control system must be provided and properly maintained over all DECD information assets according to their classification. No user shall bypass any security controls without the approval of the Principal or Preschool Director (for schools and preschools) or the ICT Security Team Leader (for other sites).

All security and access privilege requests, establishment, change and removal must be logged to an audit trail to allow subsequent review.

Third parties, including vendors, must only be provided with access for support purposes when necessary and with management approval, and their use must be monitored.

There must be regular monitoring of the security administration function, the granting of privileged accesses and the exercise of delegated responsibilities. Refer to the DECD Standard – Management of Privileged Access.

1.3 System and Applications Software Security

An adequate level of security must be maintained over operating systems and utilities, systems software, and application systems and associated information in all ICT environments.

1.4 Event Logging

Adequate audit logs, recording selected system activity and other security related events, must be activated to assist in possible investigations and to allow access control monitoring. Log data must be appropriately protected, managed and retained.

Logs must be regularly reviewed at a frequency consistent with the risk of infection and the classification of the information involved.

1.5 Security Requirements Analysis and Specification

Appropriate security, access control provisions authorisation procedures and compliance with applicable legislation must be considered in all information systems within DECD. Such aspects must be considered in the design stage of information systems, and when enhancements are specified for existing information systems.

All applicable statutory, regulatory and contractual requirements must be defined and documented for each information system, including the specific controls and responsibilities to meet these requirements.

1.6 User Identification

Users of DECD computer systems must be identified by a unique user identifier (user-id). The use of shared group user-ids will only be used in special circumstances, and only after approval from the Principal or Preschool Director (for schools and preschools) or ICT Security Team Leader (for other sites).

Vendor supplied user-ids and guest accounts must be removed or disabled, or have their default password changed.

Personal user-ids must not be shared between people and any group user-ids must not be shared with people outside the approved group of users.

All user-ids must be protected by a secure password or other approved mechanism.

All users will be accountable for any actions undertaken by their personal user-id.

1.7 Passwords

Passwords must not be words found in a dictionary, or based on anything somebody else could easily guess or obtain using person-related information (e.g. names, telephone numbers of dates of birth). Passwords must be kept confidential and not displayed or written down in any form.

Users must change passwords at regular intervals, based on the classification of the information being protected, and whenever there is an indication of possible system or password compromise.

Systems should require users to change initial passwords at their first log on.

Passwords must not be included in log on scripts or other automated log on processes.

Users must not disclose their personal password to any other person. Where users are authorised to use group user-ids, the password must not be disclosed to unauthorised people.

1.8 Data Encryption

Data encryption must be used to provide security for confidential or sensitive information depending on the risks of disclosure, operational costs and technical considerations.

1.9 Information Transport, Storage and Transmission

Adequate security must be maintained over information during transport and storage, whether in electronic or non-electronic form, to ensure there is no unauthorised disclosure or damage. The risks and consequences of unauthorised or accidental release of sensitive or confidential information must be assessed when transmitting information by facsimile, email or any other insecure means.

1.10 Mobile Computing

Portable PCs and other computing equipment which is used outside the office environment is subject to security controls, over and above those which apply within the DECD environment, to recognise the increased risk involved. Controls for mobile computing are to be based on the classification of information assets at risk. Refer to the DECD Standard – Mobile Communication Devices Security.

1.11 Access Administration

Access reports will be regularly produced to facilitate compliance to security requirements and internal control procedures.

1.12 Acceptable Use Policies

DECD staff must use ICT resources in an appropriate and professional manner according to the Code of Conduct published by Commissioner for Public Employment. Acceptable use policies must be in place for all users, including staff and students. Such policies must be in the form of a written agreement, signed by staff, students and/or their parents/guardians (as appropriate), outlining the terms and conditions of use of DECD ICT facilities, and of online behaviour and access privileges, and consequences of non-compliance.

Acceptable use policies must be reinforced through regular reminders to users.

For more information, refer to the DECD Standard - Acceptable Use Policies for Schools, Preschools & Children's Services Sites.

1.13 Segregation of Duties

Where appropriate, conflicting duties must be segregated to reduce the risk of accidental or deliberate system misuse, damage or fraud.

2. ICT Network Security

Mechanisms must be in place to provide both protection and accountability in the use of DECD networks.

2.1 Connection to External Networks

Connection of DECD networks or computers to external networks and the Internet must only be established if appropriate auditing and security barriers exist between DECD and external networks. Such connections must only be established with the express permission of the ICT Security Team Leader.

School services that are made available over the Internet must be designed with security in mind to mitigate risks to a level that is acceptable based on a risk assessment, by complying with the DECD Standard – DMZ Application Security and DECD Standard – School DMZ Server Security

2.2 Connection from External Networks

Connection of any external individual's or organisation's ICT equipment to the DECD network must only be established with the express permission of the Principal or Preschool Director (for schools and preschools) or ICT Security Team Leader (for other sites).

2.3 Network Connection Capabilities

Network connection capabilities (both internal and external) must be limited to those based on documented business requirements, and must be approved by the ICT Security Team Leader.

2.4 Malicious Software Protection

All DECD computing assets must be protected from malicious software, including computer virus infection. Regular checking for malicious software must be undertaken throughout the network and its components consistent with the risk of infection and the classification of the information involved.

Data from personal, public or other external sources must not be loaded or operated on either personal DECD computers or the DECD network without being checked for malicious software.

2.5 Network Integrity

The transfer of information must not affect the integrity of any other system's information, by avoiding the access controls established within the other system or within the network.

2.6 Capture of Network Traffic

Network devices or software designed to capture and/or analyse network traffic must not be installed on DECD networks without appropriate authorisation from the ICT Security Team Leader.

2.7 School Network Design

School and preschool networks must comply with the DECD Standard – School ICT Network Security.

2.8 Wireless Networks

School and preschool networks must comply with the DECD Standard – School ICT Network Security. Other locations must comply with the DECD Standard – Wireless Networks at DECD Corporate Sites.

2.9 Development and Operational Facilities

Development, test and operational ICT facilities must be appropriately separated to minimise the chances of impacting production systems and information.

The transfer of software and applications from development to operational environments must follow defined and documented processes.

3. ICT Physical Security

Adequate security must be provided to ensure the protection of the physical ICT and records management environments. Physical access to the ICT environment and sensitive areas must be restricted in order to protect the confidentiality, integrity and availability of information systems, information and resources.

The ICT environment and sensitive areas must be protected from damage from any relevant natural or other disaster including fire, flood and explosion.

Sensitive areas include but are not limited to computer operations areas, air conditioning, power control panels and supply, network facilities, risers, tape and disc libraries, remote sites, back-up sites, transport facilities and storerooms etc.

These requirements apply in DECD managed ICT environments and where ICT environments are managed by an external service provider. Where managed by an external service provider, DECD is responsible for identifying the required control measures that must be implemented. The control measures must be agreed with the external service provider and included in the negotiated contract.

Refer to the DECD Standard – Removable Computer Media for additional requirements on protecting DECD information stored on removable media.

3.1 Site Security

The physical work environment, all service areas and the building perimeter must have adequate facilities and access controls to prevent damage, interference and unauthorised physical access where confidential or more sensitive information or systems are involved.

3.2 Physical Access

Physical access to the ICT environment and sensitive areas must be restricted and granted only to authorised personnel with the need to access those areas in accordance with their responsibilities in the course of their duties, and taking into account relevant health and safety regulations and standards. Access rights to sensitive areas must be reviewed and updated on at least an annual basis, and evidence of the review retained.

Access to sensitive areas by third parties, including vendors, visitors and maintenance personnel must be authorised, strictly controlled, recorded and supervised.

3.3 Removal of DECD Property

DECD ICT equipment, information or software must not be taken off-site without appropriate authorisation. Where appropriate, removal and subsequent return of DECD property should be logged.

3.4 Off-site Equipment Security

DECD ICT equipment and associated media must be adequately protected from unauthorised access, manipulation, damage and theft at all times, both within and outside DECD premises.

Adequate security must be employed over equipment or media removed for repair, disposal or sale from DECD or external premises of authorised users or third parties.

DECD ICT security policies apply equally to equipment when it is off-site. Appropriate controls must be placed on off-site equipment taking into account the classification of the information on the equipment.

3.5 Information Transport/Storage

Adequate security must be maintained over information during transport and storage, whether in electronic or non-electronic form, to ensure there is no unauthorised disclosure or damage.

3.6 Clear desk policy

When not in use, printouts containing sensitive information must be locked away in suitable security furniture, preferably in a lockable drawer, cabinet or safe and with the key removed from the lock and appropriately secured. Printouts containing sensitive information must be cleared from printers immediately. Care must also be taken with printed information around photocopiers and facsimile machines.

3.7 Resigned/Terminated Users

Users who have resigned or terminated their contracts or ceased duties at DECD sites must be assessed as to their ongoing need for access to the information systems or facilities. Access can only continue with the permission of the Principal or Preschool Director (for schools and preschools) or ICT Security Team Leader (for other sites).

3.8 Dismissed/Disciplined Users

Users who have been dismissed or been subject to disciplinary action or criminal charges which may compromise the security of information systems must not have access to the DECD ICT environment, systems or facilities except with the express permission of the appropriate Executive Director or Director and the Chief Information Officer, ICT Services.

3.9 Personal Computer Facilities

Personal computers, portable equipment and associated media must be adequately protected from unauthorised access, manipulation, damage and theft at all times, both within and outside DECD premises.

Personal computers and computer terminals must be protected by password protected screensavers, or equivalent controls, when not in use or when unattended. Such settings must be automatically activated, and not rely on user activation.

3.10 Equipment Disposal and Re-use

ICT equipment which is to be re-used must be cleared of sensitive information prior to being used for another purpose. All ICT equipment, including damaged equipment, must be disposed of according to the DECD Instructions for Salvage and Disposal.

4. Email Security

Mechanisms must be in place to provide protection and accountability in usage of electronic mail (email).

4.1 Data Encryption

Data encryption must be used when sending sensitive email to recipients on foreign networks or at external locations. ICT Services will provide advice on the tools and options available relating to such encryption.

4.2 Systems Software

Access to system software and data must be granted to mailbox administrators and operations users for the purpose of system maintenance and backups.

4.3 Use of Email

Users of DECD ICT facilities will use email in an appropriate and professional manner as per the DECD Policy – Email Access and Use.

5. Internet Security

Mechanisms must be in place to provide both protection and accountability in the use of the Internet.

5.1 Malicious Software Protection

Software must be installed that automatically protects against malicious software threats from the Internet.

5.2 Use of the Internet

Users of DECD ICT facilities will use the Internet in an appropriate and professional manner as per the DECD Policy – Internet Access and Use.

6. ICT Security Awareness

Mechanisms must be in place to ensure DECD staff are aware of the importance of ICT security and its relevance in their employment, and to properly react and deal with ICT security incidents and weaknesses.

6.1 Security Organisation

DECD leadership will promote ICT security within their areas of responsibility through appropriate commitment and resources, and the reviewing and monitoring of information security policy and initiatives. Within corporate DECD this will be managed through the reviewing, monitoring and sponsorship to the Corporate Executive Team of information security policy and initiatives.

6.2 Staff Induction

All new permanent and temporary employees, consultants and contractors engaged by DECD must be provided with training and appropriate documentation about the requirements of DECD ICT security policies.

6.3 User Training

All users of DECD ICT facilities must be provided with appropriate security awareness training. This training will minimise ICT security risks and ensure that users are equipped to support DECD ICT security policies in the course of their use of DECD ICT facilities. User awareness will be supported by regular updates.

6.4 DECD Responsibilities

ICT Services will develop procedures to provide adequate information, training and assistance to employees on security issues, requirements and responsibilities.

6.3 Review of Information Security

The implementation of ICT security policies in DECD must be reviewed at least annually.

7. ICT Security Incidents

DECD will have mechanisms in place to properly react and deal with ICT security incidents and violations, both intentional and unintentional.

7.1 Disciplinary Process

DECD managers, Principals and Directors are responsible for administering the appropriate disciplinary action in their area of responsibility according to DECD human resources policies and procedures.

7.2 Reporting ICT Security Weaknesses and Incidents

All ICT security weaknesses and incidents, whether suspected or actual, must be reported as documented in the DECD Procedure – How to report an ICT Incident or Threat within DECD. Users must follow the directions of TKMS staff. Users must not attempt to prove or exploit a suspected ICT security weakness.

ICT security incidents include (but are not limited to):

- software malfunction, for example virus attacks
- hardware and software faults;

- theft or suspected theft of any DECD resources, equipment or information;
- a breach of security resulting in internal fraud or suspected fraud;
- a breach of security resulting in non-compliance with statutory requirements regarding privacy of information in legislation.

7.3 Violations

Unintentional or intentional violations of security policies and procedures must be subject to appropriate remedial advice and training, or disciplinary action according to DECD human resources policies and procedures. Users who deliberately or repeatedly violate security provisions must have their access privileges suspended until the appropriate remedial action has been determined.

7.4 Copyright Violations

Users who install, store or use illegal, unapproved or copied software will be subject to appropriate disciplinary action.

7.5 Learnings

The Corporate Executive Team must be advised of all security breaches and subsequent actions taken. ICT Services will quantify and monitor the volumes and costs of ICT security weaknesses and incidents.

7.6 Collection of Evidence

Appropriate processes must be followed to ensure that adequate evidence is available in support of actions against a person or organisation, and that the quality and completeness of such evidence is maintained.

7.7 School DMZ Environment

Schools must implement security incident management processes to ensure that incidents associated with services hosted in the school DMZ network are reported immediately to DECD central management, who will coordinate the investigation and response, as per the DECD Standard – School DMZ Security Incident Management.

8. Remote Access Security

Mechanisms must be in place to provide both protection and accountability in the use of DECD remote access services.

8.1 Authorisation

Only remote access services approved by ICT Services shall be used within DECD.

All requests for use of DECD remote access facilities must be authorised by the appropriate Principal or Preschool Director (in schools and preschools), or Executive Director or Director (for other DECD sites).

8.2 Access Route

All remote access connections must pass through the DECD security infrastructure systems. Connections which bypass the DECD security infrastructure systems (e.g. direct connections to internal modems) are prohibited.

8.3 Authorised Equipment

Only DECD owned equipment shall use DECD remote access facilities. Personal equipment must not be used on DECD remote access facilities due to the increased risks to DECD information, without the express permission of the Principal or Preschool Director or their delegate (in schools and preschools) or the ICT Security Team Leader (for other DECD sites).

8.4 Malicious Software Protection

Remote access clients must be protected against malicious software through the installation of antivirus and firewall software. Mechanisms must be established to ensure antivirus software is updated as soon as new versions become available.

9. Scope

This policy applies to all DECD ICT services and facilities.

10. Non-compliance with this Policy

Violations of this policy, depending on severity and nature, may result in reprimand, loss of ICT privileges, or termination of employment.

11. Definitions

In the context of this policy

- 'confidentiality' means ensuring that information is only available to those authorised to have access.
- 'integrity' means safeguarding the accuracy and completeness of information and software.
- 'availability' means ensuring that information and vital ICT services are available when required.
- DECD is used to include all DECD sites including preschools, schools and corporate offices.
- The term 'user' includes any person granted access to DECD ICT facilities or services located at any DECD site. This includes employees, members of the community, contractors and external parties granted access for ICT support.
- The term 'information asset' means any data or information, as well as related equipment that contains or processes data or information, that is relevant to DECD functions.
- DMZ means 'demilitarised zone' – an area of an IT network which sits between a trusted internal network, such as a DECD network, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as web and email servers.

12. References

The following departmental and whole of government policies, standards and procedures are relevant and must be read in conjunction with this policy:

- GICT/P4.1 Security – Information Security Management Framework (published by DAIS)
- DECD Information Management Policy – Privacy and Confidentiality
- DECD Instructions for Salvage and Disposal
- DECD Standard – Information Security Management System
- DECD Standard – Mobile Communication Devices Security
- DECD Standard – School ICT Network Security
- DECD Standard – School DMZ Security Incident Management
- DECD Standard – School DMZ Server Security
- DECD Standard – DMZ Application Security
- DECD Standard – Management of Privileged Access
- DECD Standard – Removable Computer Media
- DECD Standard – Acceptable Use Policies for Schools, Preschools & Children's Services Sites
- DECD Standard – Wireless Networks at DECD Corporate Sites
- DECD Policy – Internet Access and Use
- DECD Policy – Electronic Mail Access and Use
- DECD Policy – Corporate ICT Change Management
- DECD Policy – Corporate ICT Asset Management
- DECD Procedure – How to report an ICT Incident or Threat within DECD
- Code of Ethics for the South Australian Public Sector

Status:	*Final*	***File details:***
Issued:	*February 2011*	***ICT Services***
Version:	*Version 1.7*	***DECD Policy – ICT Security***
Authority:	*Corporate Executive Team* *August, 2005*	
Owned by:	*Assistant Director, ICT Infrastructure and Support Services*	
Author:	*Jenny Verner*	
Compliance:	*Mandatory*	
Review Date:	*January 2014*	