ICT Security Policy

Policy No.# ICT PAG/16-12

Effective: June 2017

VICTORIA State Government | Education and Training

Published by the Information Technology Division
Department of Education and Training
June 2017

This document is available at:
https://edugate.eduweb.vic.gov.au/sites/i/pages/production.aspx#/app/content/2575/policies_(corporate)%252Finformation_technology%252Fict_security_policy

Contents

ICT Security Policy

ICT Security Policy

1. Purpose

1.1 The purpose of this policy is to set out and communicate the Department of Education and Training's (the Department's) commitment to and requirements for, Information and Communications Technology services (ICT) security. The security requirements defined within this policy will help ensure that:

- Sensitive information is kept confidential and protected from unauthorised disclosure or interception.
- Information is accurate and complete.
- ICT is available when required.

2. Scope

2.1 This policy applies to anyone with authorised access to the Department's ICT resources regardless of work location, including but not limited to:

- Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs).
- eduGate (intranet), extranet.
- Department email systems, computer systems, software.
- Servers, desktop computers, printers, scanners.
- Portable computers, leased notebook computers, mobile phones.
- Portable storage devices (including digital cameras, USB memory sticks) and hand-held devices (such as personal digital assistants and smartphones).

2.2 This policy applies to both the corporate and school environments. However, the following sections of the policy largely do not apply to the school environment and principals should make a risk-based decision on which practices to adopt:

- Section 9 Physical and environmental security
- Section 10 Communications and operations management
- Section 11 Access control
- Section 12 Information systems acquisition, development and maintenance.

2.3 This policy does not apply to students.

3. Responsibilities

a. This policy will be communicated to all personnel.

b. All persons are accountable for their access to, and use of, ICT resources, consistent with the Acceptable Use Policy.

c. Management will ensure that information security measures are appropriate to the value of the assets and the threats to which they are exposed.

d. Management will take steps to be aware of and address all legal, regulatory, and contractual requirements pertaining to information assets.

e. Management will review required access levels for their staff.

f. Technical staff will ensure that this policy and supporting best practices and procedures are understood and implemented to address all aspects of information security.

g. The Information Management and Technology Committee (IMTC) will approve changes to this policy.

h. The Department's Executive Director, Information Technology Division (ITD) will endorse changes to this policy.

i. The Department's Manager, Risk Management & Compliance, ITD will review this policy periodically.

4. Definitions

4.1 The following definitions are applicable:

Term	Definition
Department	Department of Education and Training
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IFSG	Infrastructure & Finance Services Group
IMTC	Information Management and Technology Committee
ISO	International Organisation for Sandardisation
ITD	Information Technology Division
VPDSS	Victorian Protective Data Security Standards

5. Security Policy

5.1 The Department's ICT Security Policy selectively draws on security standard ISO/IEC 27002:2006.

5.2 This policy identifies the security requirements that the Department considers necessary to reduce security risks to an acceptable level. The requirements are grouped into the following categories:

- organisation of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development and maintenance
- information security incident management
- business continuity management
- compliance.

5.3 The policy does not provide implementation guidance for each security requirement. For advice about implementation, contact the Manager, Risk Management & Compliance, ITD via the Service Gateway: (http://servicedesk.education.vic.gov.au/).

6. Organisation of information security

6.1 *The Department's objective to effectively and efficiently manage information security will be supported by the following practices:*

a. Management will actively support security within the Department through clear direction, demonstrated commitment, explicit assignment and acknowledgment of information security responsibilities.

b. Information security activities to be co-ordinated by representatives from different parts of the organisation with relevant roles and job functions.

c. All information security responsibilities must be clearly defined.

d. Requirements for confidentiality or non-disclosure agreements that reflect the Department's needs for the protection of information must be identified and reviewed regularly.

e. Maintain appropriate contacts with relevant authorities.

f. Maintain appropriate contacts with special interest groups or other specialist security forums and professional associations.

g. The Department's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) must undergo regular independent review, including when significant changes to the security implementation occur.

The Department's objective to maintain the security of Departmental information and processing facilities when accessed or managed by external parties will be supported by the following practices:

h. The risks to the Department's information and information processing facilities from business processes involving external parties will be identified and appropriate controls implemented before granting access to external parties.

i. Security requirements will be identified and addressed before granting external users access to Departmental ICT assets.

j. Agreements with external parties, who will access, process, communicate or manage the Department's information or information processing facilities, or add products or services to information processing facilities will cover all relevant security requirements.

7. Asset management

7.1 *The Department's objective to achieve and maintain appropriate protection of Departmental ICT assets will be supported by the following practices:*

a. All assets must be clearly identified and an inventory of all important assets must be maintained.

b. All information and assets associated with information processing facilities must have a designated owner.

c. Rules for acceptable use of information and assets associated with information processing facilities must be identified, documented, and implemented.

d. Information must be classified in terms of its value, legal requirements, sensitivity, and how critical it is to the Department.

e. An appropriate set of procedures for information labelling and handling must be developed and implemented in accordance with the classification scheme adopted by the Department.

8. Human resources security

8.1 *The Department's objective that employees, contractors and external users understand their ICT security responsibilities and are suitable for their roles will be supported by the following practices. They will reduce the risk of theft, fraud or misuse of facilities.*

a. Security roles and responsibilities of employees and contractors must be defined and documented.

b. Background verification checks must be carried out on all successful candidates for employment and contracting in accordance with relevant laws, regulations and ethics. These checks must be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

c. As part of their contractual obligation, employees and contractors must agree and sign the terms and conditions of their employment contract. Contracts must state their and the Department's information security responsibilities.

The Department's objective that employees, contractors and external users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support Departmental policy in the course of their normal work will be supported by the following practices. They will reduce the risk of human error.

d. Managers must require employees, contractors and external users to apply appropriate security in accordance with established policies and procedures of the Department.

e. Employees and applicable contractors and external users will receive appropriate information security awareness training and regular updates about Departmental policies and procedures relevant to their job function.

The Department's objective that employees, contractors and external users exit the Department or change employment in an orderly manner will be supported by the following practices:

f. Employees, contractors and external users must return Departmental assets in their possession when their employment, contract or agreement ends.

g. Employee, contractor and external users' access rights to information and information processing facilities must be revoked when their employment, contract or agreement ends. Access rights must be adjusted if these contracts or agreements change.

9. Physical and environmental security

9.1 *The Department's objective to prevent unauthorised physical access, damage, and interference to Departmental premises and information assets will be supported by the following practices:*

a. Security perimeters or barriers, such as walls, card-controlled entry gates or staffed reception desks, must be used to protect areas that contain information processing facilities.

b. Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

c. Access to offices, rooms, and facilities will be controlled by appropriate physical security.

d. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster must be designed and applied.

e. Physical protection and guidelines for personnel working in secure areas must be designed and applied.

The Department's objective to prevent loss, damage, theft or compromise of assets and interruption to the Department's activities will be supported by the following practices:

f. Equipment must be housed or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

g. Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.

h. Power and telecommunications cabling that carries data or supporting information services must be protected from interception or damage.

i. Equipment must be correctly maintained to ensure continued availability and integrity.

j. Off-site equipment must be secure taking into account the different risks of working outside the Department's premises.

k. Sensitive data and licensed software must be securely overwritten or removed from storage media prior to disposal.

l. Equipment, information or software must not be taken off-site without prior authorisation.

10. Communications and operations management

10.1 *The Department's objective for correct and secure operation of its information processing facilities will be supported by the following practices:*

a. Operating procedures for information processing facilities must be documented, maintained, and available to all users who need them.

b. Changes to information processing facilities and systems must be controlled.

c. Duties and areas of responsibility for information processing facilities must be segregated to reduce opportunities for unauthorised, unintentional modification or misuse of the Department's information assets.

d. Information facilities for development, test, and production activities must be separated to reduce the risks of unauthorised access or changes to production systems.

The Department's objective to implement and maintain the appropriate level of information security and service delivery in line with external party service delivery agreements will be supported by the following practices:

e. Security controls, service definitions and delivery levels must be included in the service delivery agreements with external providers.

f. The services, reports and records provided by external providers must undergo regular monitoring, review and audit.

The Department's objective to minimize the risk of system failures will be supported by the following practices:

g. The use of system resources must be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

h. Acceptance criteria must be established for new information systems, upgrades and versions. Appropriate system tests must be carried out during development and before acceptance is signed off.

The Department's objective to maintain the integrity and availability of software and information will be supported by the following practices:

i. Detection, prevention and recovery controls to protect against malicious code must be implemented.

j. Backup copies of information and software must be taken and tested regularly in accordance with Departmental policy.

k. Networks must be managed and controlled to protect against threats and to maintain the security of systems and applications that use the network. This includes protecting information in transit.

The Department's objective to dispose of media securely and safely when no longer required will be supported by the following practices:

l. Formal procedures must be followed so that media is disposed of securely and safely when no longer required. Staff should ensure that all material on media before disposal is treated in accordance with the Department's Records Management Policy.

m. Procedures for handling and storing information must be established to protect information from unauthorised disclosure or misuse.

n. System documentation must be protected against unauthorised access.

The Department's objective to maintain the security of information and software exchanged within the Department and with an external entity will be supported by the following practices:

o. Formal exchange policies, procedures and controls must be in place to protect the exchange of information via all types of communication facilities.

p. Agreements must be established for exchanging information and software between the Department and external parties.

q. Media containing information must be protected against unauthorised access, misuse or corruption when transported beyond the Department's physical boundaries.

r. Information in electronic messages must be protected appropriately.

s. Policies and procedures must be developed and implemented to protect information associated with the interconnection of business information systems.

The Department's objective for secure electronic commerce services will be supported by the following practices:

t. Information involved in electronic commerce passing over public networks must be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification.

u. Information involved in on-line transactions must be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

The Department's objective to detect unauthorised information processing activities will be supported by the following practices:

v. Audit logs recording user activities, exceptions and information security events must be produced and retained for an agreed period to assist in future investigations and access control monitoring.

w. Procedures for monitoring the use of information processing facilities must be established and the results of the monitoring activities must be reviewed regularly.

x. Logging facilities and log information must be protected against tampering and unauthorised access.

y. Activities of system administrators and system operators must be logged.

z. Faults must be logged, analysed, and appropriate must be action taken to address.

aa. The clocks of all relevant information processing systems within an organisation or security domain must be synchronised to a common time source.

11. Access control

11.1 *The Department's objective to ensure authorised user access and to prevent unauthorised access to information systems will be supported by the following practices:*

a. A formal user registration and de-registration procedure must be in place for granting and revoking access to information systems and services.

b. The allocation and use of privileges must be controlled.

c. The allocation of passwords must be controlled through a formal management process.

d. Management must follow a process to review users' access rights at regular intervals.

The Department's objective to prevent unauthorised user access, and compromise or theft of information and information processing facilities, will be supported by the following practices:

e. Users must follow good security practices in the selection and use of passwords.

f. Users must ensure that unattended equipment has appropriate protection.

g. Users must adopt a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.

The Department's objective to prevent unauthorised access to networked services will be supported by the following practices:

h. Users must only be given access to services they are specifically authorised to use.

i. Appropriate authentication methods must be used to control remote access by users.

j. Physical and logical access to diagnostic and configuration ports must be controlled.

k. Network segmentation is used to restrict access and improve performance. Groups of information services, systems and users with similar security, access and performance requirements must be segregated on the network.

l. For shared networks, especially those extending across the organisation's boundaries, the capability of users to connect to the network shall be restricted.

m. Routing controls should be implemented for networks to ensure that computer connections and information flows are limited to those required for business and security purposes.

The Department's objective to prevent unauthorised access to operating systems will be supported by the following practices:

n. Access to operating systems must be controlled by a secure log-on procedure.

o. All users must have a unique identifier (UserID) which only they can use.

p. Systems for managing passwords must be interactive and must ensure quality passwords.

q. Software that is capable of overriding system and application controls must be restricted and tightly controlled.

r. Inactive sessions must automatically shut down after a defined period of inactivity.

s. Restrictions on connection times must be used to provide additional security for high-risk applications.

12. Information systems acquisition, development and maintenance

12.1 *The Department's objective to ensure that security is an integral part of information systems will be supported by the following practice:*

a. Documented business requirements for new information systems, or enhancements to existing information systems, must specify the requirements for security controls.

The Department's objective to prevent errors, loss, unauthorised modification or misuse of information in applications will be supported by the following practices:

b. Data input to applications must be validated to ensure it is correct and appropriate.

c. Validation checks must be incorporated into applications to detect corruption of information through processing errors or deliberate acts.

d. Requirements to ensure authenticity and protection for message integrity in applications must be identified. Appropriate controls must also be identified and implemented.

e. Data output from an application must be validated to ensure correct and appropriate processing of stored information.

The Department's objective to protect the confidentiality, authenticity or integrity of information by cryptographic means will be supported by the following practice:

f. Key management must be in place to support the Department's use of cryptographic techniques.

The Department's objective to ensure the security of system files will be supported by the following practices:

g. Procedures must be in place to control the installation of software on production systems.

h. Test data must be selected carefully, and protected and controlled.

i. Access to program source code must be restricted.

The Department's objective to maintain the security of application system software and information will be supported by the following practices:

j. Changes must be implemented following formal change control procedures.

k. When operating systems are changed, business critical applications must be reviewed and tested to ensure there is no adverse impact on organisational operations or security.

l. Modifications to software packages shall be discouraged, limited to necessary changes, and all changes must be strictly controlled.

m. Outsourced software development must be supervised and monitored.

The Department's objective to reduce risks resulting from exploitation of published technical vulnerabilities will be supported by the following practice:

n. Timely information about technical vulnerabilities of information systems must be obtained and appropriate controls implemented to address the associated risks.

13. Information security incident management

13.1 *The Department's objective to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken will be supported by the following practices*:

a. Information security incidents must be reported in line with the Department's ICT Security Incident Policy (https://edugate.eduweb.vic.gov.au/sites/i/pages/production.aspx#/app/content/2576/policies_(corporate)%252Finformation_technology%252Fict_security_incident_policy).

b. All employees, contractors and external users of information systems and services must note and report any observed or suspected security weaknesses in systems or services.

The Department's objective to ensure a consistent and effective approach is applied to the management of information security incidents will be supported by the following practices:

c. Management responsibilities and procedures must be established and followed to ensure a quick, effective and orderly response to information security incidents.

d. Mechanisms must be in place to enable the types, volumes and costs of information security incidents to be quantified and monitored.

e. Evidence must be collected and retained where follow-up action is required against a person or organisation after an information security incident involving legal action (either civil or criminal).

14. Business continuity management

14.1 *The Department's objective to counteract interruptions to business activities and to protect critical business processes from the effects of failures of information systems or disasters will be supported by the following practices:*

a. A managed process, that addresses the information security requirements needed for the Department's business continuity, must be developed and maintained for business continuity throughout the Department.

b. Events that can cause interruptions to business processes must be identified, along with the probability and impact of these interruptions and their consequences for information security.

c. Plans must be developed and implemented to maintain or restore operations and ensure availability of information after interruption to, or failure of, critical business processes. These plans must include the required level of availability and time scales.

d. Business continuity plans must be coordinated for consistency. Each plan must address information security requirements and identify priorities for testing and maintenance.

e. Business continuity plans must be tested and regularly updated to ensure they are up to date and effective.

15. Compliance

15.1 *The Department's objective to avoid breaches of any law, statutory, regulatory or contractual obligations will be supported by the following practices:*

a. For each information system, the Department must explicitly define, document and update all relevant statutory, regulatory, and contractual requirements and our approach to meet these requirements.

b. The Department must implement appropriate procedures to ensure compliance with legislative, regulatory, and contractual requirements for intellectual property rights and on the use of proprietary software.

c. Important records must be protected from loss, destruction and falsification in accordance with statutory, regulatory, contractual, and business requirements.

d. Data must be protected to ensure privacy as required by relevant legislation, regulations, and contracts.

e. Users shall be deterred from using information processing facilities for unauthorised purposes.

f. Cryptographic controls must be used in compliance with all relevant agreements, laws, and regulations.

The Department's objective to ensure compliance with Departmental and Victorian Government security policies and standards will be supported by the following practices:

g. Managers must ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

h. Information systems must be regularly checked for compliance with security implementation standards.

i. Applications and supporting infrastructure recorded in the Department's Critical Application list will be security-tested at least annually, and

- after a major security incident involving the application or system; or
- following a major change to the system configuration, setup or technology; or
- following a change in support or outsourcing arrangements.

The Department's objective to maximise the effectiveness of the information systems audit process will be supported by the following practices:

j. Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimize the risk of disruptions to business processes.

k. Access to information-system audit tools must be protected to prevent misuse or unauthorised access.

16. Legislative/Business Context

16.1 The Victorian Government's Information Security Management Framework document SEC/STD/01 required the Department to have an information security policy or equivalent.

16.2 This framework lapsed when the Victorian Protective Data Security Standards (VPDSS) was published. The VPDSS is required to be implemented by July 2018.

16.3 This policy will be updated to align with the VPDSS once its standards have been fully adopted by the Department.

17. Privacy and Human Rights

17.1 This policy is consistent with the Information Privacy Act 2000.

17.2 This act has been superseded by the Privacy and Data Protection Act 2014. The Data Protection Act requires the VPDSS to be implemented.

17.3 This ICT Security Policy will be updated once the standards from the VPDSS have been fully adopted by the Department.

17.4 This policy has been checked for compliance with the Charter of Human Rights and Responsibilities Act 2006.

18. Related Documents

18.1 This policy is to be read in conjunction with the following Departmental and Divisional documents:

- Acceptable Use Policy for ICT Systems (http://www.education.vic.gov.au/school/principals/infrastructure/Pages/acceptableuse.aspx).
- ICT Security Incident Policy (https://edugate.eduweb.vic.gov.au/sites/i/pages/production.aspx#/app/content/2576/policies_(corporate)%252Finformation_technology%252Fict_security_incident_policy).
- Portable Storage Device Security Policy (https://edugate.eduweb.vic.gov.au/sites/i/pages/production.aspx#/app/content/2580/policies_(corporate)%252Finformation_technology%252Fportable_storage_device_security_policy)
- Records Management Policy (https://edugate.eduweb.vic.gov.au/sites/i/pages/production.aspx#/app/content/2581/policies_(corporate)%252Fdata_and_information_management%252Frecords_management_policy)
- Password Policy

  (https://edugate.eduweb.vic.gov.au/sites/i/pages/production.aspx#/app/content/2579/policies_(corporate)%252Finformation_technology%252Fpassword_policy)

19. Contact

19.1 Direct your queries about this policy to the Manager, Risk Management & Compliance, ITD via the Service Gateway (https://www.eduweb.vic.gov.au/servicedesk).

20. Review

20.1 This policy will be reviewed every 24 months or earlier if necessary.

21. Approving Authority

21.1 Changes to this policy may not be invoked without prior approval by the Information Management and Technology Committee.