Procedure

Information security

Audience

Version effective: 02/01/2020
Version: 1.1

Department-wide

Purpose

This procedure provides all ICT users with their obligations to protect the department's information and data against loss or inappropriate release, and secure ICT assets, devices, services and business systems against unauthorised use, accidental modification and information security incidents.

Overview

The department develops, implements, maintains and continually reviews appropriate security controls and processes in compliance with Queensland Government's information security related policy, leading ICT security processes and practices, reporting and auditing requirements, and legislative instruments.

Employees are accountable to protect the department's information and data against loss or inappropriate release by applying information security classifications and secure ICT assets, devices, services and business systems against unauthorised use, accidental modification and information security incidents.

Responsibilities

Employees

- Protect and secure the department's information and ICT business systems by accepting responsibility for the availability, integrity and confidentiality of information in their care.
- Abide by the department's Use of ICT facilities and devices guideline and the Code of Conduct for the Queensland Public Service when using ICT systems and devices.

Supervisors, managers, directors, principals or above

- Ensure their employees are aware of their obligation to protect and secure the department's information and ICT business systems.
- Ensure the requirements of this procedure are implemented within their business unit.

System security administrators with ICT security responsibilities within the department

- Manage and coordinate activities and resources to prevent, detect, remove, report and respond to incidents of malware and malicious code.

Cyber Security and Identity Management, Information and Technologies Branch

- Provide departmental support and controls for ICT security across departmental ICT business systems and assets.

Enterprise Technology Solutions, Information and Technologies Branch

- Monitor the system's capacity to ensure the risks of system overload or failure that could lead to a security breach are avoided.

Process

ICT security

The department develops, documents, implements, maintains and continually reviews appropriate security controls and processes to comply with Queensland Government's policy, leading ICT security practices, reporting and auditing requirements, and legislative obligations.

The Information security guideline and the iSecurity intranet website provide employees with guidance on ICT security compliance with Queensland Government's Information security policy (IS18:2018).

To ensure that the department's information is protected against loss or inappropriate release, the department complies with the Queensland Government information security classification framework (QGISCF) by applying the appropriate information security classification:

- **OFFICIAL**: Represents the department's non-sensitive information, of a routine nature.
- **SENSITIVE**: Confidential information, of medium sensitivity, where access is to be restricted to authorised persons on a 'need to know' basis.
- **PROTECTED**: Confidential information, of high sensitivity, that requires a substantial degree of protection.

Where the department receives and holds information that is owned/created by another government agency the department maintains the classification applied by the owning/creating agency.

Applying information security classifications

Employees must apply an information security classification to information they create, process or manage in accordance with the different classifications as outlined in the Information security classification and handling guideline to identify, protect and secure information.

When managing information, **employees** that create, process or handle information must ensure:

- electronic documents have an information security classification displayed on the front page, in a watermark, or the header or footer, and in the accompanying metadata, or document properties
- any changes to the information security classification is made through a formal approval process that involves the owner and/or custodian
- the information security classification applied to an information item is not changed when the item is transferred to another location or between ICT business systems

- removable media (e.g. CDs, DVDs, USB devices, hard drives, SD cards) that contains information classified as SENSITIVE or PROTECTED is destroyed or not used for other purposes without being securely wiped or rendered unusable
- reasonable precautions are taken to protect information (based on its information security classification) against unauthorised access, illegal or unauthorised use, disclosure, modification, duplication, disruption and/or destruction.

Protecting information

Employees must protect and secure the department's information and ICT business systems by:

- ensuring that any departmental information they create, manage and store is protected from unauthorised access or amendment where the information security classification is SENSITIVE or PROTECTED
- protecting SENSITIVE or PROTECTED information from unauthorised access by maintaining a clear screen and locking the ICT device when unattended.

Supervisors, managers, directors, principals or above must:

- establish business unit or school security control processes including roles and responsibilities for handling and managing of any SENSITIVE or PROTECTED, and incorporate these into position descriptions and performance agreements
- provide appropriate induction and on-going ICT security training for employees such as the Information Security module of Keys to managing information (DoE employees only) (mandatory on induction) and iSecurity intranet site
- ensure that an annual internal review of ICT security practices, including a risk assessment, is undertaken.

Cyber Security and Identity Management, Information and Technologies Branch must:

- Establish
    - processes to periodically review and test firewall rules and associated network architectures to ensure the expected level of network perimeter security is maintained
    - processes to periodically review and update current network security design, configuration, vulnerability and integrity checking to ensure network level security controls are appropriate, effective and up-to-date
    - security controls for ICT business systems, network infrastructure and applications
    - security controls during all stages of system development, as well as when new systems are implemented and maintained in the operational environment.
- Ensure
    - system change and release management processes include confirmation that appropriate security controls have been applied and the capacity requirements of the system have been considered
    - appropriate change control, acceptance and system testing, planning and migration control measures are being adhered to when upgrading or installing software in the operational environment
    - accurate system security records show traceability from original business requirements to actual configuration and implementation, including appropriate justification and authorisation.

- Develop
    - the department's network security policy and network security control definitions for the internal or external exchange of information
    - security controls to manage all aspects of online and internet activities including anonymity/privacy, data confidentiality, use of cookies, applications/plug-ins, practices for downloading executable code, web server security configuration, auditing, access, encryption.
- Implement
    - processes to manage software vulnerability risk for all ICT business systems, network infrastructure and applications
    - maintenance processes that provide appropriate protection of the ICT network's underpinning and ancillary services from internal and external threats (e.g. mail gateways, domain name resolution, time, reverse proxies, remote access and web servers)
    - a patch management program for operating systems, firmware and applications of all ICT assets to maintain vendor support, increase stability and reduce the likelihood of threats being exploited.
- comply with the department's network security policy and network security control definitions for information exchange (internally or externally)
- periodically perform penetration testing for all critical online services
- address security requirements in all stages of new ICT systems, network infrastructure and applications
- create and manage Secure Sockets Layer (SSL) Certificates.

Enterprise Technology Solutions will:

- synchronise all ICT assets to a trusted time source that is visible and common to all
- develop, maintain and test business continuity and ICT disaster recovery plans and processes for ICT business systems under their control in accordance with the department's Business continuity management (BCM) procedure
- in consultation with Director, Information and Governance Management provide a recommendation to Assistant Director-General, Information and Technologies whether to notify affected individuals where a security breach has resulted in unauthorised access to personal information.

Malware and malicious code prevention

The department installs and monitors antivirus software to prevent, detect, remove, record and report computer viruses and malware attacks or malicious code activity.

All ICT users must not:

- disable or interfere with the operation of antivirus software
- download software from the internet unless authorised by their supervisor, manager, teacher or above. If appropriate, scan downloaded software for malware and malicious code. For technical assistance, contact the Services Catalogue Online (SCO) (DoE employees only)

- develop, distribute or run any computer programs or code that is intended to replicate itself, cause damage, and/or impede the performance of any computer, software application or network whether malicious or otherwise.

All ICT users must:

- connect departmentally-owned ICT devices approved for work use to the network for antivirus software updates at least weekly
- exercise caution when opening unexpected email and related attachments
- scan all files and information contained on mobile media and storage devices for malware and malicious code prior to being used on any department ICT device. Scanning can be either manual or automated
- isolate infected devices by either turning off or disconnecting the network cable, where possible
- report any malware and/or malicious code attacks to their supervisor or manager.

System security administrators with ICT security responsibilities within the department must:

- establish and implement a mandatory procedure for scanning to ensure that traffic entering and leaving the department's network is appropriately scanned for malicious or unauthorised content
- define and conduct vulnerability/integrity scans of core software to ensure detection of unauthorised changes
- ensure departmentally-approved antivirus software has been installed on all specified corporate and school ICT devices, is configured to the department's specifications and is regularly updated with new definition files
- ensure that service level agreements with ICT service providers who manage school computers contain provisions whereby antivirus software is installed and regularly updated.

Breach of security

All ICT users accessing departmental computers, tablets, laptops, and mobile devices via the departmental networks that breach and/or bypass the information security malware and malicious code prevention measures may be subject to:

- Restriction and/or suspension of access privileges and disciplinary action.
- Where users within the community have been identified as having breached and/or bypassed the information security malware and malicious code prevention measures, access rights will be withdrawn. The matter may be reported to state or federal police as part of the ICT security investigation process.
- Users may be called upon to explain any incident.

Reporting ICT security incidents

Employees must report any ICT security incident to their **supervisor, manager, principal or above** (as appropriate) who will follow the steps below:

Step 1: Resolve the incident locally, if possible.

Step 2: If the incident cannot be resolved locally, submit an Information Security – Report an Incident (DoE employees) or contact the following (as appropriate):

- for technology issues contact IT Service Centre on 1800 680 445 or Services Catalogue Online (SCO) (DoE employees only)
- Ethical Standards for violations of the Queensland Government's Code of Conduct for the Queensland Public Service.

Definitions

All ICT users	Departmental corporate (central and regional offices) and school employees, students and users in the community who use the department's ICT facilities and devices that access business systems, networks and services such as internet, telephone, email, printer, Wi-Fi etc. in accordance with the Use of ICT systems procedure.
ICT security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of an ICT business system or the information stored, processed or communicated by an ICT business system.

Legislation

- *Financial Accountability Act 2009* (Qld)
- Financial and Performance Management Standard 2019 (Qld)

Delegations/Authorisations

- Nil

Related policies

- Queensland Government Enterprise Architecture policies and standards
- Information and Communication Technology (ICT) (DoE employees only)
- Queensland Government's Information security policy (IS18:2018)
- Queensland Government information security classification framework (QGISCF)
- Code of Conduct for the Queensland Public Service

Related procedures

- Use of ICT systems
- Implementing a business continuity plan

Guidelines

- Information security classification and handling guideline
- Information security guideline

Supporting information/websites

- Keys to managing information (DoE employees only)
- iSecurity
- Information security – Report an incident (DoE employees)
- Services Catalogue Online (SCO) (DoE employees only)

Contact

For further information, please contact:

- Information and Governance Management
  Information and Technologies Branch (I&T Branch)
  Email: InformationManagement@qed.qld.gov.au

Review date

01/06/2020

Superseded versions

Previous seven years shown. Minor version updates not included.

1.0 Information security
1.0 Information Management (IM)
1.0 Information Communication and Technology (ICT)
2.0 Classification and handling of information assets*
    1.0 IFM-PR-003: Classification and handling of information assets
4.0 Maintaining the security of department information and systems*
    2.0 IFM-PR-006: Maintaining the security of department information and systems
4.0 Malware and malicious code prevention*
    3.0 Malware and malicious code prevention

* indicates procedures replaced by the Information Management and Information Communication and Technology procedure in 2014.

Creative Commons Licence