**Information security guideline**

***Document details***

|  |  |
| --- | --- |
| **Item** | **Description** |
| Document title | Information Security Guideline |
| Reference | 15/377334 |
| Publication coordinator | ICT Sustainability, ITB |
| Date of completion | 31/07/2017 |
| Status | Draft |
| Copy number | V5.0  |

***Revisions***

|  |  |  |
| --- | --- | --- |
| **Version** | **Date of change** | **Reason for change** |
| V5.0 | July 2017 | Increased focus on security controls.Restructure of headings and format for ease of use. |
| V4.0 | 7 April 2014 | Complete rewrite to reduce content. Changed wordings to reflect new ICT Procedure that replaced the Maintaining the Security of Department Information and Systems Procedure and with a focus on how the department will implement the IS18's mandatory clauses. Name changed from Information Security Implementation Advice on Mandatory Clauses V3.0 to Information Security Guideline (TRIM 14/33019).Endorsed by Information Steering Committee on 20 February 2014 and by the Executive Management Board on 7 April 2014. |
| V3.0 | n/a | *Details not available.* |
| V2.0 | August 2012 | Added IS18 Information Security Standard V5 Mandatory Clauses and minor updatesTrim ref. 12/242720 (Attachment to IFM-PR-006 with Trim ref. 11/236682 and later DETE Information Security Management Policy (TRIM 12/204490)). |
| V1.0 | 15/01/2010 | Approved IFM-PR-006 Implementation Advice Trim No. 10/169614. |

***Information security classification***

The audience for this guideline is the employees of the Department of Education and Training only. It has an information security classification of Public. It is published to the internet within the Policy and Procedure Register as part of the department's proactive release of information under the [*Right to Information Act 2009* (Qld)](https://legislation.govnet.qld.gov.au/LEGISLTN/CURRENT/R/RightInfoA09.pdf). Readers external to the department are to understand that many links will not be available for their use. Any requests for further information can be made under a formal [Right to information and information privacy application](http://deta.qld.gov.au/right-to-information/make-a-request.html).

***Review and update***

This guideline will be reviewed and revised to reflect departmental changes or any major change in business directions and objectives, or at least annually.



<http://creativecommons.org/licenses/by/3.0/au/>

© State of Queensland (Department of Education, Training and Employment) 2017

##

## Table of contents

[Introduction 4](#_Toc488412545)

[1. Policy, planning and governance 4](#_Toc488412546)

[2. Asset management 6](#_Toc488412547)

[3. Human resource management 7](#_Toc488412548)

[4. Physical and environmental management 8](#_Toc488412549)

[5. Communications and operations management 10](#_Toc488412550)

[6. Access management 12](#_Toc488412551)

[7. System acquisition, development and maintenance 14](#_Toc488412552)

[8. Incident reporting 16](#_Toc488412553)

[9. Business continuity management 17](#_Toc488412554)

[10. Compliance management 19](#_Toc488412555)

[Common information security terms 20](#_Toc488412556)

# Introduction

This guideline supports the [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure by providing details of employee responsibilities to ensure they understand and adhere to information security requirements within the department for the acquisition, handling and disposal of all departmental information, information assets and ICT business systems.

The Department of Education and Training undertakes information security planning and implementation through specified and targeted information security business operations and the day-to-day activities of all employees. These activities are guided by Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) and are articulated through the department's [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure and this document. The information within this document is structured to support compliance with IS18's *Information Security Policy* – Mandatory Clauses v1.0.2.

The aim of this document is to provide all departmental employees with guidance and resources to easily fulfil their responsibilities with respect to information security.

All employees have a responsibility to ensure they understand and adhere to information security requirements within the department for the acquisition, handling and disposal of all departmental information, information assets and ICT business systems.

The advice provided here-in is a guide to assist in understanding and operationalising information security within business units and schools. This advice does not replace any specific responsibilities or operations required as part of defined information security role descriptions within the department. Business units and schools should use this guide in conjunction with their area's existing information security processes.

# Policy, planning and governance

## Aim

Policy, planning and governance with appropriate practices and processes in place ensures information security remains an integral consideration in all aspects of departmental operations.

## Rationale

The department has adopted the following policy documentation to communicate and govern information security requirements to its employees[[1]](#footnote-1):

* Information Security Framework[[2]](#footnote-2)provides a high-level outline and direction on the main aspects the department is required to implement to ensure secure information and ICT business systems.
* [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure articulates key aspects of the department's information security requirements.
* Information Security Plan[[3]](#footnote-3)provides guidance over a two year period on aspects of whole of government compliance that requires further action (including reviewing, strengthening etc.). Business areas with specific deliverables within this plan have approved this commitment and are implementing these actions.
* A mandatory induction module within the [Keys to managing information](https://det.qld.gov.au/workfordet/induction/queenslandstateschools/Documents/mandatory-annual-training-ready-reckoner.pdf) course on information security.
* course on information security.

## Roles and responsibilities

**All employees**

All departmental employees have a responsibility to ensure they adhere to information security policies/procedures within the department.

## Controls

* Departmental employees **must** comply with the [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedureand all supporting documentation.

## Resources

* OnePortal's [Information security](https://oneportal.deta.qld.gov.au/services/informationtechnology/informationsecurity/Pages/default.aspx) (DET employees only) web page provides a quick overview of key information security advice.
* The [School security](https://ppr.qed.qld.gov.au/pp/school-security-procedure) procedure identifies responsibilities and recommended strategies regarding security management of physical assets in schools.
* [Stay Smart Online](http://www.staysmartonline.gov.au/) website is an Australian Government website that provides information for safe internet use to protect your personal and financial information online.
* *Information Security Plan*provides the requirements placed on the department to protect and secure the department's information and information assets.
* Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.

## Further advice

If you have any questions in relation to information security policy, planning and governance please contact ICT Sustainability, Digital Transformation, Information and Technologies Branch (ITB) by emailing ICT.Sustainability@det.qld.gov.au.

# Asset management

## Aim

Physical and environmental controls are in place to ensure the confidentiality, integrity and availability of information and information assets in accordance with their information security classification.

## Rationale

Information assets are an identifiable collection of data stored in any manner and are recognised as having value for the purpose of enabling the department to perform its business functions e.g. files, databases, paper-based and electronic documents, records, hardware items, software or other infrastructure items.

## Roles and responsibilities

## All employees

Every employee is responsible for ensuring information assets remain secure.

**Information asset custodians**

Information asset custodians are responsible for the security of information assets they have oversight of.

## Controls

## Employees must apply an information security classification to information or information assets they create in accordance with the [Information asset and recordkeeping](https://ppr.qed.qld.gov.au/pp/information-asset-and-recordkeeping-procedure) procedure.

## Employees must determine appropriate means of information handling, storage, transfer and disposal commensurate with the information security classification.

## Information asset custodians must ensure an appropriate level of security is employed for information assets they have carriage of.

## Employees must report security incidents where information security has been – or is likely to be – breached.

## Employees must report all suspicious emails and inappropriate online behaviour immediately to their supervisor, manager, principal or above.

## Resources

## [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure provides employees with direction on the correct classifying, labelling and handling of information assets, which are owned, managed or handled by the department and its service providers.

## Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.

## Further advice

For further advice on information asset management contact Information Management, Digital Transformation, Information and Technologies Branch (ITB) by emailing InformationManagement.INFOMNGT@det.qld.gov.au.

# Human resource management

## Aim

Employees are appropriately authorised to access sensitive or confidential departmental information.

## Rationale

The department implements pre, during and post-employment processes including security checks, awareness raising and secure controls across the employment lifecycle[[4]](#footnote-4).

## Roles and responsibilities

## Directors

## While recruiting employees, Directors of business area are to determine and approve the information security requirements of the position and have the appropriate details outlined in the position advertisement and role description[[5]](#footnote-5).

## When recruiting employees, ensure all new employees undergo a Criminal History check.

**Managers**

* Managers are ensure their employees are provided with induction (including the department's mandatory course [Keys to managing information](https://det.qld.gov.au/workfordet/induction/queenslandstateschools/Documents/mandatory-annual-training-ready-reckoner.pdf), ongoing information security training and awareness raising programs that highlight the information security requirements of their role[[6]](#footnote-6).
* Human resources
* During the post-employment process, steps should be taken to ensure the security of the department's information remains by following the departmental separation procedure[[7]](#footnote-7).

**All employees**

All employees are to:

* adhere to information security requirements when undertaking operations for the department
* fully understand and operationalise any additional information security operations specific to their role
* adhere to information security requirements across their entire employment life style.

## Controls

* All employees **must** undertake the mandatory induction training on [Keys to managing information](https://oneportal.deta.qld.gov.au/services/humanresources/projects/Professionaldevelopment/keystomanaginginformation/Pages/default.aspx) (DET employees only), which includes an information security module.

## Resources

* [Criminal history checks](https://ppr.qed.qld.gov.au/pp/criminal-history-check-procedure) procedure outlines the procedure to conduct criminal history checks on current and intending employees.
* [Employee separation](https://ppr.qed.qld.gov.au/pp/employee-separation-procedure) procedure outlines the requirements on managers, principals and employees when ceasing employment with the department, including the return of departmental property, revocation of the network and ICT device access, and finalisation of outstanding finance and administrative matters.
* [State Schools Division's (formerly Education Queensland's) role descriptions](http://education.qld.gov.au/hr/recruitment/role-descriptions/index.html) web page for the department provides all approved role descriptions including any security requirements.
* OnePortal's [human resources forms, tools and templates](https://oneportal.deta.qld.gov.au/Services/HumanResources/Forms/default.aspx) web page includes role descriptions, workforce planning and induction documents.
* Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.

## Further advice

If you have any questions in relation to information security requirements for human resource management contact Human Resources Branch by emailing Recruitment.HUMANRES@det.qld.gov.au.

# Physical and environmental management

## Aim

Physical security measures are applied to facilities and network infrastructure to protect systems.

## Rationale

Physical controls should be put in place for buildings, identified secure areas and equipment. The level of control placed within an area (e.g. secure locked, security pass access) is defined by the information security classification assigned to the information and physical assets housed in the area or location[[8]](#footnote-8). Guidance on this is available within the [Queensland Government Information Security Classification Framework](http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2417-queensland-government-information-security-classification-framework) (QGISCF).

## Roles and responsibilities

**All employees**

All employees are responsible for:

* ensuring they only access secure areas and use equipment that they have been approved to do so within their position
* maintaining secure building entries, including ensuring secure doors close behind themselves and unauthorised people do not enter these areas
* correctly handling departmental equipment according to the specific information security classification requirements.

**Information custodians**

Information custodians are responsible for ensuring information assets are classified correctly and apply the appropriate ICT physical and environmental controls.

## Controls

* All employees **must** follow building and secure area controls to ensure that only authorised personnel are allowed access.
* All unattended computers **must** be locked (clear screen).
* All X-In-Confidence, Protected and Highly Protected documents **must** be properly secured (clear desk policy).
* Employees **must** secure departmentally-owned mobile devices when leaving their desk for extended periods. Appropriate security measures include locking equipment in filing cabinets, drawers or cupboards, and using security cable/s lockdowns.
* Employees **must not** have sensitive or classified conversations in public areas (including on mobile phones) within earshot of those without a need-to-know.
* Employees **must not** leave departmentally-owned mobile devices in cars. If this is not possible, lock the mobile devices in the boot. In station wagons and vans, employees can safeguard mobile devices by placing it out of sight of passers-by. Do not leave mobile devices in cars overnight or for long periods of time or during extreme cold or hot weather.
* When travelling, employees **must not** check-in departmentally-owned laptops as under-carriage baggage when travelling by air, rail or bus
* Employees **must** retain control of departmentally-owned laptops when passing through security checkpoints at airports. Maintain sight of the laptop when it is passing through security scanners or being inspected by security personnel.
* Employees **should** be cognisant of their surroundings when performing work on mobile devices or laptops in public areas.
* When travelling, employees **should** secure laptops in a hotel safe rather than the room itself, if possible. If this is not possible store the laptop in a lockable cupboard, drawer or suitcase, or at least out of sight.

## Resources

* [Asset maintenance](https://ppr.qed.qld.gov.au/pp/asset-maintenance-and-school-swimming-pool-operation-procedure) procedure identifies responsibilities for the Asset Maintenance Program (AMP) and Special Maintenance Programs (SMP) for the department's facilities.
* [Equipment management for business units](https://ppr.qed.qld.gov.au/pp/equipment-management-for-business-units-procedure) procedure provides the department's procedure for acquisition, recording, stocktake, loan and disposal (write-off) of departmental equipment, within business units.
* [Equipment management for schools](https://ppr.qed.qld.gov.au/pp/equipment-management-for-schools-procedure) procedure provides the department's procedure for acquisition, recording, stocktake, loan and disposal (write-off) of departmental equipment, within schools.
* [School security](https://ppr.qed.qld.gov.au/pp/school-security-procedure) procedure identifies responsibilities and recommended strategies regarding security management of physical assets in schools.
* School Security Program's [Security Design Requirements](https://oneportal.deta.qld.gov.au/Services/Facilities/Forms/Documents/Security-Design-Guidelines.pdf) (DET employees only) for use in the designing and upgrading of new school buildings.
* [School Security for ICT Hardware Guide](https://oneportal.deta.qld.gov.au/Services/Facilities/Forms/Documents/SecurityforICThardware.pdf) (DET employees only) provides an overview for purchasing and managing ICT hardware within schools. Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.

## Further advice

If you have any questions in relation to information security policy, planning and governance please contact ICT Sustainability, Digital Transformation, Information and Technologies Branch (ITB) by emailing ICT.Sustainability@det.qld.gov.au.

# Communications and operations management

## Aim

Communications practices and governance are conducted in a secure manner.

## Rationale

The department documents and implements operational procedures and controls (such as capacity planning, application integrity, backups, network security (including aligning with the Queensland Government's [Network Transmission Security Assurance Framework](http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2401-network-transmission-security-assurance-framework) (NTSAF) guidelines[[9]](#footnote-9)), media handling, information exchange and ecommerce) for all information and information assets processing facilities[[10]](#footnote-10). They are to be managed securely and consistently, in accordance with the level of security required[[11]](#footnote-11).

These responsibilities are also to be captured through contracts or agreements with companies and organisations that provide third party service delivery for the department, including ICT procurement and equipment management[[12]](#footnote-12).

## Roles and responsibilities

**All employees**

All employees are responsible for:

* handling and managing any information, information asset and/or ICT business system according to its [information security classification](https://ppr.qed.qld.gov.au/pp/information-security-procedure)to Information Security Procedure] and the [Information security classification and handling guideline](https://isecurity.education.qld.gov.au/staff/information-security/how-to-classify-information)
* ensuring they are aware of and adhere to all information security operations (access controls, data backup, etc.) and purchasing procedures
* understanding the risks with malicious code when using the internet and/or connecting devices to the department's network
* using the [Government Information and Technology Contracting](https://www.forgov.qld.gov.au/new-ict-contracting-framework) (GITC) Framework for contract specifications and engaging GITC approved suppliers[[13]](#footnote-13).

## Controls

* All employees **must** be aware of and adhere to all departmental information security and purchasing procedures.
* When contracting for service delivery through a third party (external to the department) **should** use [GITC](http://www.hpw.qld.gov.au/supplydisposal/GovernmentProcurement/GITCFramework/Pages/default.aspx) approved suppliers.
* Backup cycles and procedures **must** be reviewed and updated relative to the business risk, frequency with which data and software is modified and the criticality of the system to the department's operations. This includes the following at a minimum:
* incremental and full weekly backups of all data, operating system and applications
* the complete operating system on a monthly basis.
* Employees **must** handle different media formats according to the [Information security classification and handling guideline](https://isecurity.education.qld.gov.au/staff/information-security/how-to-classify-information).

## Resources

* [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure provides the requirements placed on employees to protect and secure the department's information and ICT business systems.
* [Asset maintenance](https://ppr.qed.qld.gov.au/pp/asset-maintenance-and-school-swimming-pool-operation-procedure) procedure identifies responsibilities for the Asset Maintenance Program (AMP) and Special Maintenance Programs (SMP) for the department's facilities.
* [Purchasing and procurement](https://ppr.qed.qld.gov.au/pp/purchasing-and-procurement-procedure) for purchasing goods and services from suppliers external to the department and funded by departmental or school bank accounts, regardless of the source of those funds (including for example, funds from students, parents and fundraising). Excludes real property transactions but includes capital works and infrastructure.
* OnePortal’s [PurchaseIT](https://oneportal.deta.qld.gov.au/Services/Procurement_Purchasing/PurchaseIT/Pages/default.aspx) (DET employees only) is an online shopping tool which allows easy comparison of suppliers, specifications, prices and warranty information – available to all employees. The product range includes desktops, laptops, printers, hardware accessories and Apple computers. Ordering is undertaken through the department's finance systems, [OneSchool](http://education.qld.gov.au/smartclassrooms/working-digitally/oneschool.html) and [SAP](https://oneportal.deta.qld.gov.au/SERVICES/FINANCE/SAP/Pages/default.aspx) (DET employees only).
* [State procurement policy](http://www.hpw.qld.gov.au/SiteCollectionDocuments/QLDProcurementPolicy.pdf) provides guidance on maximising value for money and reducing the costs of procurement across Queensland Government.
* OnePortal's [software load, performance and security testing services](https://oneportal.deta.qld.gov.au/Services/Procurement_Purchasing/Supplyarrangements/ict-testing-security-services/Pages/default.aspx) (DET employees only) lists the department's approved suppliers under DETPSA-100788 for load, performance, testing and security/penetration testing.
* [Government Information and Technology Contracting (GITC) Framework](https://www.forgov.qld.gov.au/new-ict-contracting-framework) provides standard contractual terms and conditions for use and acquisition of ICT products and/or services.
* Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.
* Queensland Government's [Procurement and Disposal of ICT Products and Services – IS13](http://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2501-procurement-and-disposal-of-ict-products-and-services-is13) information standard provides the principles applicable to the acquisition, management, maintenance and disposal of ICT products and services across the Queensland Government. A supporting [guide](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/3359-is13-implemenation-guideline) provides an overview of the ICT procurement process.

## Further advice

If you have any questions in relation to information security requirements for communications and operations management contact ICT Sustainability, Digital Transformation, Information and Technologies Branch (ITB) by emailing ICT.Sustainability@det.qld.gov.au.

# Access management

## Aim

Access to departmental information and ICT business systems are maintained through risk mitigation, controlled user access and authentications[[14]](#footnote-14).

## Rationale roles and responsibilities

**All employees**

Employees are provided access to the department's ICT business systems, with authorisation from their direct supervisor. Employees should always be aware of the level of access they are allowed. This also applies to students, parents, members of Parent and Citizens Associations and community groups, with approval sought through the school principal.

Where employees have departmental information and/or information assets they are information custodians or information owners of, departmental procedures for approving access to these assets must be followed. Additionally, only allow employees with a need-to-know should be granted access to the information.

## Controls

* User access rights **must** be in accordance with the requirements of the business process being undertaken and will be authorised by the user's responsible supervisor.
* User access **must** only be provided on a 'need-to-know' basis.
* Privileged users **must** strictly adhere to the level of security related to the information asset and ICT business system they have access. Breach of the granted access level will be reported and investigated.
* User ID and passwords **must not** be disclosed to another individual even if requested. Never lend your system access to another person, even to your manager or a trusted colleague. Do not respond to emails requesting your personal information, user ID or password (especially if claiming to be from your ICT or IT administration employees), and never respond to emails requesting your banking or financial details.
* Network user passwords **must** be reset every 60 days. User passwords can be changed by pressing the CTRL+ALT+Delete keys then selecting 'Change a password' or use the [Self Service Password Reset (SSPR) system](https://passmgt.deta.qld.gov.au/PasswordReset/default.aspx) to reset a password. Alternatively, password reset requests can be made by phoning the Service Centre on phone 1800 680 445. Validation of requests will be conducted when required.
* Strong passwords **must** be chosen. A strong/secure password:
* is at least 8-characters long
* does not exceed 32-characters, and
* at a minimum contain at least:
* one upper and lowercase character e.g. a-z, A-Z
* one digit e.g. 0-9
* one punctuation character e.g.!@#$%^&\*()\_+|~-=\`{}[]:";'<>?,.

One source for developing a secure password is the [Microsoft website](http://www.microsoft.com/security/online-privacy/passwords-create.aspx).

* Employees **must** ensure passwords used to gain access to a personal mobile device are unique i.e. not the same as those used for gaining access to the departmental network or encrypting/decrypting sensitive folders or files on that device.
* Multi-functional devices **must** have an approved appropriate security locking mechanism, based on a security risk assessment to prevent intrusion of the system.
* Media, including any removable media such as memory sticks and external USB memory drives that contains departmental information **must** be protected against unauthorised access, misuse or corruption in accordance with the [Queensland Government Information Security Classification Framework](http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2417-queensland-government-information-security-classification-framework) (QGISCF) during use and transportation beyond the department's physical boundaries.
* For advice on mobile device configuration contact the Service Centre on phone 1800 680 445 or via Service Centre Online.
* Remote access:
* Management processes **must** include registering all persons with remote access privileges, logging all remote access attempts and activities, and ensuring all users are authenticated before access to the network is granted.
* Using departmental devices and personal mobile devices **must** require appropriate authorisation (refer to [Use of mobile devices](https://ppr.qed.qld.gov.au/pp/use-of-mobile-devices-procedure) procedure
* Devices used for remote access:
* Laptops **must** be configured according to the department's managed operating environment (MOE) to meet requirements for encryption, authentication and security locking including session time-outs.
* For personal mobile devices, business requirements and a risk assessment **must** meet [Queensland Government Authentication Framework](http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2415-queensland-government-authentication-framework) (QGAF) requirements for encryption, authentication and security locking including session time-outs. At a minimum, the device will need to meet the department's security requirements (see [iSecurity](https://isecurity.education.qld.gov.au/) intranet site for details) at a minimum installing, running and updating anti-virus software[[15]](#footnote-15).
* All wireless communications **must** include appropriate configured product security features that is equivalent to or of higher level to the security of wired communications.
* Network connections of all devices used for remote access **must** be cancelled upon termination of employment and can be revoked at any time.

## Resources

* [Use of ICT systems](https://ppr.qed.qld.gov.au/pp/use-of-ict-systems-procedure) procedure outlines that the department provides access to its information resources based on the information security classification of the system/content. The department provides secure access to information in departmental ICT business systems to authorised users through the provision of electronic identities.
* [Use of ICT systems](https://ppr.qed.qld.gov.au/pp/use-of-ict-systems-procedure) procedure advises all departmental network users of their responsibilities and the consequences of their behaviour when using the department's network and related systems, and provides guidelines for ensuring the accountability, transparency and safe operation of the network.
* Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.

## Further advice

For further advice to request access to the department's ICT network, contact the [Service Centre Online](https://qlddet.service-now.com/sco/) or the Service Centre on 1800 680 445.

For further policy advice contact ICT Sustainability, Digital Transformation, Information and Technologies Branch (ITB) by emailing ICT.Sustainability@det.qld.gov.au.

# System acquisition, development and maintenance

## Aim

Systems are acquired, developed and maintained in a manner that safeguards the system against information loss, theft and unauthorised disclosure.

## Rationale

During ICT business system acquisition, development and maintenance activities are undertaken to determine security controls, cryptographic controls, protection of system files, prevent errors, loss, unauthorised or misuse of information, and activities that reduce risks arising from the exploitation of technical vulnerability.

## Roles and responsibilities

**All employees**

ICT business system acquisition, development and maintenance is mainly coordinated and controlled within the Information and Technologies Branch (ITB). Employees where possible, are to utilise the department's ICT network and systems to undertake the department's business processes.

**Business units and schools**

Where individual business units or schools acquire, develop and maintain an ICT business system to fulfil a specific business process of the department, they will follow the departmental information security procedures and will be required to operate these systems to the standard set out for all State Government departments in [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security).

## Controls

* Project and program managers **must**, prior to undertaking a project to acquire or develop an ICT business system, refer to the OnePortal's [Portfolios, programs, project and advice](https://team.oneportal.deta.qld.gov.au/sites/P3O/default.aspx) website.
* ICT business system project management documentation **must** include security controls (OnePortal's [Portfolios, programs, project and advice](https://oneportal.deta.qld.gov.au/Services/InformationTechnology/ICTServiceCatalogue/ICTProjectsAndAdvice/Pages/ICTProjectsAndAdvice.aspx)) and be implemented through-out system development.
* System owners **must** ensure audit logs that are kept and security controls for segregation of the ICT business system adhere to [Queensland Government Information Security Controls Standards](http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2431-queensland-government-information-security-controls-standard) (QGISCS)[[16]](#footnote-16).
* Clear security intrusion detection and incident reporting processes **must** be outlined as part of project development and deployment.
* System owners **must** ensure cryptographic controls comply with Queensland Government's [Network Transmission Security Assurance Framework](http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2401-network-transmission-security-assurance-framework) (NTSAF) guidelines[[17]](#footnote-17). The NTSAF outlines that the primary goal of cryptographic controls is to conceal data to protect it against unauthorised third-party access by applying encryption.

## Resources

* [Purchasing and procurement](https://ppr.qed.qld.gov.au/pp/purchasing-and-procurement-procedure) procedure for purchasing goods and services from suppliers external to the department and funded by departmental or school bank accounts, regardless of the source of those funds (including for example funds from students, parents and fundraising). Excludes real property transactions but includes capital works and infrastructure.
* [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure provides the requirements placed on employees to protect and secure the department's information and ICT business systems.
* Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.

## Further advice

For further advice on the acquisition, development and maintenance of an ICT business system, contact the [Service Centre Online](https://qlddet.service-now.com/sco/) or phone 1800 680 445.

For further project management advice contact ICT Sustainability, Digital Transformation, Information and Technologies Branch (ITB) by emailing ICT.Sustainability@det.qld.gov.au.

# Incident reporting

## Aim

Appropriate mechanisms are in place for the reporting and management of information security incidents.

## Rationale

The department implements end-to-end information security incident management processes. Network and system outages and issues are published when they occur on the homepage of [Service Centre Online](https://qlddet.service-now.com/sco/)[[18]](#footnote-18).

Internally, the department will undertake event weakness reporting (through the security incident register) and a clear escalation (and where required investigation) process. The department will report suspected breach activity and information security incidents to the relevant authority. The escalation process will include Internal Audit, Ethical Standards Unit and/or Legal and Administrative Law Branch, with any official misconduct cases being reported to relevant regulatory authorities.[[19]](#footnote-19)

Breaches of information security that result in unsatisfactory audit and employee reports can lead to disciplinary action (including dismissal) and/or action by relevant regulatory authorities. Disciplinary action and process is determined under the [*Public Service Act 2008* (Qld)](https://legislation.govnet.qld.gov.au/LEGISLTN/CURRENT/P/PublicServA08.pdf)where relevant.

## Roles and responsibilities

**All employees**

Every employee of the department is responsible for reporting ICT security incidents and suspected security incidents. Reporting of security incidents you become aware of can be escalated through your direct supervisor, using the [Information security incident online reporting form](https://oneportal.deta.qld.gov.au/Services/InformationTechnology/informationsecurity/Pages/default.aspx) (DET employees only), calling the [ICT Service Centre](https://qlddet.service-now.com/sco/) or emailing infosec@det.qld.gov.au.

**System Owners**

ICT system owners are responsible for ensuring security testing is undertaken for vulnerability management and security breaches (including detectable intrusions).

## Controls

## Employees must report information security incidents through their direct supervisor, using the [Information security incident online reporting form](https://oneportal.deta.qld.gov.au/Services/InformationTechnology/informationsecurity/Pages/default.aspx) (DET employees only), calling the [ICT Service Centre](https://oneportal.deta.qld.gov.au/Services/InformationTechnology/ICTServiceCatalogue/ICThelp/Pages/ICThelp.aspx) or emailing infosec@det.qld.gov.au.

## Employees must comply with requests from their line management in relation to assisting with security investigations.

## Resources

* [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure section provides the requirements placed on employees to protect and secure the department's information and ICT business systems. This includes requirements for reporting information security breaches.
* Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.

## Need further advice on incident management?

If you have any questions in relation to incident management contact the [Service Centre Online](https://qlddet.service-now.com/sco/) or phone 1800 680 445.

# Business continuity management

## Aim

Business continuity management plans and processes give consideration to information security policies and controls.

## Rationale

The department has implemented an information and ICT assets business continuity plan in the event of a disaster or major security failure. This will enable the timely restoration or recovery of the affected ICT assets, with minimal disruption to departmental business.

The Information and Technologies Branch (ITB) within the department looks after business continuity planning for the department's information and ICT assets, where these fall within ITB's operational control[[20]](#footnote-20). However, all business units and schools (and the senior employees within) are responsible for ensuring, in the event of a disaster, that the information and ICT assets within their operational responsibility are able to be recovered or restored, or an alternative option for operation is deployed in a timely manner.

## Roles and responsibilities

**All employees**

Employees should be aware of their business area's business continuity plan for its ICT assets. Where employees are responsible for the custodianship of information assets, or operation of a departmental ICT business system, they are to ensure business continuity plans are in place in the event of a disaster or major service outage and that they are regularly reviewed and updated to reflect current processes, contacts and that required equipment is readily available.

**Business system owners**

* Business system owners that operate ICT business systems are responsible for ensuring security testing is undertaken for vulnerability management and security breaches (including detectable intrusions).
* Disaster recovery plans are developed, tested and updated regularly to ensure that they are up-to-date with the requirements for continuality of critical and business-as-usual operations[[21]](#footnote-21).
* Events arising from risks and vulnerabilities that can cause interruptions to business processes will be regularly identified, including the probability and impact of such interruptions and their consequences for information security.
* Risk assessment processes and plans will be maintained and risk mitigation strategies will be reviewed and updated to ensure the security of all information assets.
* Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.

## Controls

* Business continuity plans and emergency management plans **must** be reviewed on a regular basis.
* Employees **must** be trained/re-trained on business continuity plans and emergency management plans at least annually.

## Resources

* OnePortal's [business continuity management](https://oneportal.deta.qld.gov.au/Services/strategymanagement/GSP/EnterpriseRiskManagement/Pages/Businesscontinuitymanagement.aspx) web page provides details on the department's Business Continuity Management Strategy.
* OnePortal's [Emergency and Security Management Unit](https://oneportal.deta.qld.gov.au/Services/Facilities/emergencysecuritymanagementinformation/Pages/default.aspx) website provides advice on the department's emergency management policy.
* OnePortal's [software load, performance and security testing services](https://oneportal.deta.qld.gov.au/Services/Procurement_Purchasing/Supplyarrangements/ict-testing-security-services/Pages/default.aspx) lists the department's approved suppliers under DETPSA-100788 for load, performance, testing and security/penetration testing.
* [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure provides the requirements placed on employees to protect and secure the department's information and ICT business systems. This includes requirements for reporting information security breaches.

## Further information

If you have any questions in relation to information security requirements for business continuity management contact Governance Strategy and Planning by emailing enterprise.riskmanagement@det.qld.gov.au.

# Compliance management

## Aim

The department meets legislative and Whole-of-Government information security compliance obligations.

## Rationale

Employees are to comply with departmental policies and procedures, Queensland Government policy, legislative and audit requirements[[22]](#footnote-22). The department's planning and implementation controls on ICT security are governed within the Information Security Framework and Information Security Plan (see Section 1 of this guide for details).

The department provides advice on meeting these requirements through the [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure

## Roles and Responsibilities

**All employees**

Employees are responsible for:

* ensuring they are aware of information security requirements and adhere to these when undertaking operations as part of their position within the department. Reporting security incidents in accordance with Section 8 of this guide.

## Controls

## All employees must understand and comply with departmental ICT policies, procedures and supporting documents.

## Project/program managers must understand and comply with legislative and whole-of-government requirements relevant to their project.

## Resources

* [Information security](https://ppr.qed.qld.gov.au/pp/information-security-procedure) procedure provides the requirements placed on employees to protect and secure the department's information and ICT business systems. This includes requirements for reporting information security breaches.
* Queensland Government's [Information Standard - IS18](http://www.qgcio.qld.gov.au/products/information-security) provides the requirements for a consistent approach to information security implementation and operation across Queensland Government.

## Further advice

If you have any questions in relation to information security compliance management Information Management, Digital Transformation, Information and Technologies Branch (ITB) by emailing InformationManagement.INFOMNGT@det.qld.gov.au.

# Common information security terms

|  |  |
| --- | --- |
| **Control**  | A measure that is taken to mitigate risks. |
| **Encryption**  | The art or science concerning the principles, means, and methods for rendering plain information unintelligible. |
| **Firewall**  | A network device that filters incoming and outgoing network data, based on a series of rules. |
| **Hardware**  | The physical components of computer equipment including peripheral equipment. For example, personal computers, servers, laptops, printers, routers, smart phones and mobile phones. |
| **ICT asset** | ICT hardware, software, systems and services used in the department's operations including physical assets used to process, store or transmit information. |
| **ICT business system** | Information technology systems or applications designed to automate and support the undertaking of a specific business process or processes. They may create, receive, manage and maintain business information relating to business processes. |
| **Information asset** | Is an identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling the department to perform its business functions this includes transactional information in business systems, documents and mail. |
| **Information custodian** | Delegated by the information owner to set and define the rules of an information asset to ensure the information asset is appropriately managed to maintain its currency, integrity and availability. This includes identifying its information security classification/s and, registering and maintaining its details within the department's [Information Asset Register](https://detereporting.dete.qld.gov.au/sites/IAR/default.aspx). |
| **Malicious code**  | Any software that attempts to subvert the confidentiality, integrity or availability of a system. Malicious code includes: logic bombs, trapdoors, Trojan programs, viruses and worms. |
| **Media**  | The component of hardware that is used to store information. |
| **Need-to-Know** | The principle to restrict an individual’s access to only the information that they require to fulfil their role.  |
| **Privileged user**  | A user who can alter or circumvent system security protections. This may also apply to users who may have only limited privileges, such as software developers, who can still bypass security precautions. A privileged user may have the capability to modify system configurations, account privileges, audit logs, data files or applications for example, system administrators, ICT security employees, helpdesk employees. |
| **Remote access**  | Any access to a departmental practice system from a location not within the physical control of the department. |
| **Removable media**  | Storage media that can be easily removed from an ICT business system and is designed for removal for example, hard disks, CDs, floppy disks, tapes, smartcards and flashcards. |
| **Risk**  | A risk is 'a future event' that impacts on organisational objectives. It may happen or it may not. We can plan for risk based on its likelihood and potential impact – risks can be avoided completely, minimised, transferred to another party, or we can meet them head on with strategies to deal with their effects. |
| **Security incident**  | An event that impacts on the confidentiality, integrity or availability of a system through an act of unauthorised access, disclosure, modification, misuse, damage, loss or destruction. |
| **Server**  | A computer used to run programs that provide services to multiple users for example, file servers, mail servers, and database servers. |
| **System administrator**  | The person responsible for the day-to-day operation of the system. |
| **User**  | Any individual or entity accessing the department's ICT business systems and/or applications including employees, students, adults (parents/caregivers), business partners and/or the wider community. |
| **Virus** | See malicious code. |

1. Queensland Government Information Security Policy – Mandatory Clauses 1.1.1, Nov 2010, v1.0.2 [↑](#footnote-ref-1)
2. Latest copy is available through HPE Records Manager. [↑](#footnote-ref-2)
3. Latest copy is available through HPE Records Manager. [↑](#footnote-ref-3)
4. Queensland Government Information Security Policy – Mandatory Clauses 3.2.1, Nov 2010, v1.0.2 [↑](#footnote-ref-4)
5. Queensland Government Information Security Policy – Mandatory Clauses 3.1.1, Nov 2010, v1.0.2 [↑](#footnote-ref-5)
6. Queensland Government Information Security Policy – Mandatory Clauses 3.2.2, Nov 2010, v1.0.2 [↑](#footnote-ref-6)
7. Queensland Government Information Security Policy – Mandatory Clauses 3.3.1, Nov 2010, v1.0.2 [↑](#footnote-ref-7)
8. Queensland Government Information Security Policy – Mandatory Clauses 4.1.1 and 4.1.2, Nov 2010, v1.0.2 [↑](#footnote-ref-8)
9. QGCIO, Information Standard - IS18 Policy – Principal 5, Nov 2010, v5.0.0 [↑](#footnote-ref-9)
10. Queensland Government Information Security Policy – Mandatory Clauses 5.1.1, Nov 2010, v1.0.2 [↑](#footnote-ref-10)
11. Queensland Government Information Security Policy – Mandatory Clauses 5.1.2, Nov 2010, v1.0.2 [↑](#footnote-ref-11)
12. Queensland Government Information Security Policy – Mandatory Clauses 5.2.1, 5.2.2, 5.2.3, Nov 2010, v1.0.2 [↑](#footnote-ref-12)
13. Queensland Government Information Security Policy – Mandatory Clauses 5.2.3, Nov 2010, v1.0.2 [↑](#footnote-ref-13)
14. Queensland Government Information Security Policy – Mandatory Clauses 6.8.1 Nov 2010, v1.0.2 [↑](#footnote-ref-14)
15. Queensland Government Information Security Policy – Mandatory Clauses 5.4.1, 5.4.3, 6.5.3, 6.5.4 Nov 2010, v1.0.2 [↑](#footnote-ref-15)
16. Queensland Government Information Security Policy – Mandatory Clauses 7.5.2, Nov 2010, v1.0.2 [↑](#footnote-ref-16)
17. Queensland Government Information Security Policy – Mandatory Clauses 7.3.1, Nov 2010, v1.0.2 [↑](#footnote-ref-17)
18. Queensland Government Information Security Policy – Mandatory Clauses 8.1.4 Nov 2010, v1.0.2 [↑](#footnote-ref-18)
19. Queensland Government Information Security Policy – Mandatory Clauses 8.2.1 Nov 2010, v1.0.2 [↑](#footnote-ref-19)
20. Queensland Government Information Security Policy – Mandatory Clauses 9.1.2 Nov 2010, v1.0.2 [↑](#footnote-ref-20)
21. Queensland Government Information Security Policy – Mandatory Clauses 9.2.2, 9.2.3, 9.2.4 Nov 2010, v1.0.2 [↑](#footnote-ref-21)
22. Queensland Government Information Security Policy – Mandatory Clauses 10.1.1 Nov 2010, v1.0.2 [↑](#footnote-ref-22)