# Information System Operations - Procedures

/explore/policies-and-procedures/information-system-operations-procedures

## Definitions

Please refer to the University's Glossary of Terms for policies and procedures.

Terms and definitions identified in the Information and Communication Technology (ICT) Security - Managerial Policy are specific to these procedures and are critical to its effectiveness.

## 1. Purpose of procedures

These procedures support the Information and Communication Technology (ICT) Security - Managerial Policy and provide guidance on activities and responsibilities in relation to the administration and operations of the University's Information Systems.

## 2. Procedures

### 2.1 Unique identification and designation of Business System Owner for each information system

The role of Business System Owner is to be assigned to each of the University's Information Systems and will normally reside within the functional area considered most relevant in relation to the nature of the system. The Business System Owner will normally be the most senior officer or member of staff responsible for the management of a School, or a management or support service, or administrative area or sub-section which is specifically identified for allocation of funding within the University's budget framework.

An appropriate Business System Owner will be identified in consultation with appropriate stakeholders.

Where a Business System Owner cannot be readily identified, or agreed upon, recommendation will be made by the ICT Governance Committee to the Chief Operating Officer.

APPROVAL AUTHORITY
Vice-Chancellor and President

RESPONSIBLE OFFICER
Chief Operating Officer

DESIGNATED OFFICER
Director, Information Technology

FIRST APPROVED
8 August 2017

LAST AMENDED
11 January 2019

EFFECTIVE START DATE
17 August 2017

REVIEW DATE
8 August 2022

STATUS
Active

RELATED DOCUMENTS
Business Continuity Management - Governing Policy
Critical Incident Management - Governing Policy
ICT Security - Managerial Policy
Incident Management - Procedures
Social Media - Managerial Policy

RELATED LEGISLATION / STANDARDS
Queensland Information Standards

### 2.2 Information system classification

An Information System classification will be made by the Business Systems Owner in consultation with Information Management Services and Information Technology Services.

### 2.3 Monitoring the University's IT network infrastructure and addressing audit issues

The Information Technology department will monitor the University's IT network infrastructure and address related audit issues.

### 2.4 Monitoring, authorising and revoking access and addressing related audit issues

The Business System Owner will monitor, authorise and revoke user access to their assigned Information System.

The Information Technology department will assist the Business System Owner with appropriate tools and in the performance of the tasks necessary to manage Information System access.

### 2.5 Avoid breaches of legal, statutory, regulatory, contract or privacy obligations

The Business System Owner will work with Information Technology Services and other appropriate areas of the University, to ensure compliance with respect to legal, statutory, regulatory, contract or privacy compliance obligations.

Information Technology Services will assist the Business System Owner in monitoring compliance and assist in internal and/or external audits, including reporting on the status of audit issues.

### 2.6 Central Authentication system

The Information Technology department will ensure that the centralised authentication system is implemented and that only currently authorised client have access. They will facilitate access in accordance with Information System classification.

### 2.7 Maintenance of Information Security Management System

The Information Technology department will maintain the Information Security Management System.

Business System Owner will advise the Information Technology department of compliance obligations that they may be aware of which may require incorporation into the Information Security Management System in order to avoid breaches of legal, statutory, regulatory, contract or privacy obligations.

### 2.8 Policy awareness

The Business System Owner is responsible for advising University Clients of security responsibilities specific to their assigned Information System.

Information Technology Services is responsible for advising University Clients of the University's ICT Security – Managerial Policy and related procedures and other general ICT security matters.

### 2.9 Staff training

The Business System Owner is responsible for ensure that University Clients using the information System are trained in its use.

Information Technology Services is responsible for ensure that University Clients are trained in accessing the network and using IT systems.

### 2.10 Access to Information

The Business System Owner is to work with the Information Technology department and other areas of the University as appropriate to assess the risks to their assigned Information System and implement physical security measures where the system is not housed in a designated University Data Centre.

The Information Technology department will provide access to the information System, and implement and manage physical security of the system when it is housed within a Designated University Data Centre.

The Information Technology department will facilitate mechanisms for system access and authentication.

The Information Technology department will provide advice and assistance to the Business System Owner to implement physical security to systems which are not housed in a Designated University Data Centre.

### 2.11 Third Party University Clients

The Business System Owner is to ensure that third party clients sign a confidentiality agreement and are assigned the appropriate level of access to the information System.

The Information Technology department is to ensure that third parties receive access in accordance with the Information and Communications Technology (ICT) Access Control – Managerial Policy.

### 2.12 Security of the information in various media formats

The Business System Owner is to consult with Information Technology and Information Management Services to consider the security of media in various formats.

Where the use of certain media for Information Systems is Confidential or Restricted, the manner in which this is to be implemented is to be agreed.

### 2.13 Remote access to Confidential (and Restricted) Information Systems

The Information Technology department is to provide the mechanisms and infrastructure for remote access.

### 2.14 Ownership of information, data and software within the University

The Business System Owner is to consult with the Information Management Committee and Data Management Group to ensure access and use of information, data and software is assigned in a manner consistent with the University's policies and with other contracts and agreements.

### 2.15 Operations management procedures

The Business System Owner is to develop operational work instructions consistent with this procedure in order to fulfil their duties.

### 2.16 Changes to Information Systems

The Business System Owner is to make changes to their assigned Information System in accordance with established change management practices.

The Information Technology department is to maintain an overarching IT change management process to ensure the confidentiality, integrity and availability of data.

### 2.17 Segregation of Duties

The Business System Owner is to ensure Segregation of Duties exists for roles and responsibilities within the Information System and consider segregations when making changes to clients' access.

The Information Technology department is to assist in developing and maintaining Segregation of Duties within their information Systems.

## 2.18 Detection and prevention of malicious software and behaviours

The Information Technology department is to implement systems and practices to minimise the impacts of potential malicious software and activity on the University network and impacting the University's Information Systems.

## 2.19 The installation of unauthorised information and communications technology on the network

The Information Technology department is to implement systems and practices to minimise the impacts of the installation of unauthorised software and hardware on the University environment.

## 2.20 Backup of Information Systems

The Business System Owner is to advise the Information Technology department of backup requirements for their Information System.

The Information Technology department is to operate, support, maintain, and ensure the ongoing backup of Information Systems as required by Business System Owners, as well as the testing of backups and the offsite storage of backup media.

## 2.21 Appropriate activity logging

The Business System Owner is to initiate activity logging where possible and as appropriate, and periodically review the logs for anomalous activity.

Where required by an appropriate authority, the Business System Owner may be required to work with the Information Technology department and other areas with relevant compliance obligations (and the requesting authority) to review logs and on provide requested data.

The Information Technology department is to provide the means for the University to monitor and log activities performed on its Information Systems and network and to log relevant activity. As appropriate the logs are to be provided to the Business System Owner for review. Analytic tools may be used to identify and report on anomalous activity identified within the logs.

## 2.22 Information Security incidents

The Business System Owner is to inform the Information Technology department of any identified security incidents related to their Information System.

The Information Technology department is to investigate known incidents in accordance with the University's Critical Incident Management - Managerial Policy.

## 2.23 Transmission of confidential information

The Business System Owner is to use appropriate means to transmit confidential and restricted data in accordance with the Information Asset Security Classifications and Handling – Guidelines.

The Information Technology department is to provide the means for clients to transmit data in a secure matter, such as via a secured file transfer service.

## 2.24 Business continuity management

The Business System Owner is to ensure that an appropriate Business Continuity plan is developed and in place and that these are aligned with the IT Service Continuity Plan and Disaster Recovery Plan for the Information System.

The Information Technology department is to ensure that an appropriate Disaster Recovery Plan is developed and in place and that these are aligned with the Business Continuity Plan for the Information System. Refer to the Business Continuity Management - Managerial Policy and Critical Incident Management - Managerial Policy and associated procedures.

## 2.25 Information security requirements

The Business System Owner is to ensure that the Information Technology department is aware of any specific information security requirements for the business unit so they can be addressed as part of the acquisition, implementation, development or enhancement of the Information System.

The Information Technology department is to address information security requirements, including those specified by the Business System Owner, as part of the acquisition, implementation, development or enhancement of the Information System.

## 2.26 End user developed systems

University Clients are to ensure that Information Technology Services is aware and kept up to date of any End User developed applications (such as Excel spreadsheets or Access databases) used by the business unit which are being relied upon for business-critical services.

If informed of any important End User developed applications where continuity and support becomes critical, Information Technology Services is to ensure these are institutionalised and brought under the control of either the Information Technology department or the relevant business area.

## 2.27 Periodic IT Security Audits

The Business System Owner and/or Information Technology Services may be required or requested (e.g. by Internal or External auditors) to provide specific Information System data. All areas are to liaise with each other in identifying and providing the requested data.

## 2.28 Breaches of the Policy

The Business System Owner may restrict access for specific University Clients to the Information System after being instructed by a relevant authority.

Information Technology may restrict access for specific University Clients to the network after being instructed by a relevant authority.

END