

(Standard) ICT Glossary and Definitions

Document Purpose

Document Purpose	To define the meaning of glossary terms and definitions used in the ICT Policy and Standards framework.			
Document Information	Version	1.0		
	Release Date	July 2008		
	Release Status	Final		
	Review Date	July 2009		
	Author(s)	Michael Thompson		
	Owner	Principal Manager - PMIM		
	Print Date	Last Printed: 21/06/2010 12:25:00 PM		
	Approved By	Principal Manager - PMIM		
	Policy	USQ Policy for ICT Information Management and Security		
	Type of Document	Standard		
	Electronic Location and Filename	http://www.usq.edu.au/resources/ict_glossary_and_definitions.pdf		
Version Control	Version	Date	Author(s)	Summary of Changes
	0.1	2008	Michael Thompson	Document creation
	1.0	July 2008	Maggie Fryer	Final release
Error Advisory	<p>To the Reader:</p> <p>If you encounter any inaccuracies or printing faults in this document please contact the Owner (see Document Information section, above) as soon as possible. The Owner will then initiate the required modifications</p> <p>If you are unable to contact the Owner, contact that person's Manager Supervisor.</p> <p>Thank you for helping the Division of ICT Services maintain quality documentation.</p>			

Table of Contents

Document Purpose	1
Document Information	1
Error Advisory	1
1 Definitions.....	3
2 Related Documents.....	7

1 Definitions

Acceptance Criteria	Criteria defined at the commencement of a project or activity that specify the goals or conditions that must be met in order for the acquisition or creation of the specific ICT hardware, software or service.
Authentication	The ability to verify the claimed identity of an individual as established in the identification process.
Authorisation	Clients are granted rights to access a resource if they meet the criteria policed by the Resource Manager. Clients are permitted to access only those resources for which they have been authorised by a Resource Manager (see Registration and Authentication).
Availability	Ensuring that authorised clients have access to information and associated assets when and where required.
Business Continuity	Business continuity (BC) addresses organisational recovery following a disaster. It assumes that prevention arrangements have failed and that an incident has occurred which has interrupted normal business to the extent that corrective action is required.
Business Continuity Plan	A plan that describes a sequence of actions, and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation as soon as possible.
Campus Cabling	Cabling on a premises containing more than one building.
Client(s)	An authenticated member of the university community who is authorised to access a particular information and communication technology resource(s). This includes, but is not limited to: <ul style="list-style-type: none"> • all students and alumni, • academic and administrative staff, • visiting academic staff, and • external individuals or organisations
Computer Account	Combination of a unique user identifier and a password that allows an individual access to an information and communication technology resource. The account remains the property of the University and is only loaned to the client for legitimate purposes as defined in University policy.
Confidentiality	Ensuring that information is accessible only to those authorised to have access and is protected from unauthorized disclosure or intelligible interception.
Controls	A protective measure - an action, a device, a policy, a procedure, or a technique - that reduces the vulnerability of a system or a threat to that system, either preferably by preventing attacks, or other less powerful methods which only detect a breach as or after it occurs.
Corporate Executive Portfolio Steward/ Principal Activity Steward/System Sponsor	A senior member of University staff who is accountable for assigned resources. University managers include Vice-Chancellor, Deans of Faculties, General Manager, Group Managers, CTO, Heads of Centres and Directors.
Delegated Officer	As defined in the HR Policies and Procedures Manual Part A2: Delegations
DICTS	The Division of ICT Services, University of Southern Queensland.

Disaster Recovery	Disaster recovery is concerned with plans to restore ICT services if a disruptive incident occurs.
Governance	Governance refers to how the University and its various staff organisational units involved in a project or process (individually and collectively) make decisions relating to the establishment, management and control of the project or process. In practice, governance refers to the people, policies, processes and structures which enable collaborative and informed decision making.
ICT	Information and Communication Technology.
ICT Facilities and Devices	ICT facilities and devices cover computers (including palm and handheld devices); telephones (including mobiles); removable media; radios or other high frequency communication devices; television sets; digital or analogue recorders (including DVD and video); cameras; photocopiers; facsimile machines; printers (and other imaging equipment); electronic networks; internet; email; web mail; and fee-based web services.
ICT Resources	Refers to the resources the University needs to meet the informational requirements of the University and its clients, and carry out the University's operational responsibilities. Resources can include the following: <ul style="list-style-type: none"> (a) information obtained, produced or supplied by the University (b) the information systems of the University; (c) equipment or facilities that support the University's information systems (includes ICT Facilities and Devices); (d) the University's human resources.
Illicit Material	Illegal material such as child pornography.
Information	Any collection of data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form.
Information Asset	An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling the University to perform its business functions. Can include hardware, software, data and reputation.
Information Assurance	Information operations to protect information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. <p>Includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.</p>
Information Management	Information management is the means by which an organisation plans, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains and disposes of its information; as well as any means through which the organisation ensures that the value of that information is identified and exploited to its fullest extent.
Information Risk	Information risk is defined as the exposure to occurrences that will have an impact, either positive or negative, on the confidentiality, integrity and/or availability of USQ's information assets. <p>Risk arises out of uncertainty and has two elements:</p> <ul style="list-style-type: none"> • the frequency/likelihood of something happening; and • the severity/impact of the consequences arising from the event.

Information Security	Protection of the confidentiality, integrity and availability of information.
Information Technology	Management of techniques used in data handling and processing; their applications; computers and their interactions with people and machines.
Integrity	The assurance that information has been created, amended or deleted only by the intended authorised person and/or means and that the accuracy, and that the information complete and processing methods are safeguarded.
Legal Compliance	Ensuring that all legal and contractual obligations are met.
Malicious code or software	Collectively called 'malware' and consisting of computer viruses, worms, Trojan horse programs, spyware, and other malicious code - is software most often designed to damage or disrupt computer systems, or promote data loss/leakage
Owner	The term owner is the recognised officer who is identified as having the authority and accountability under the University legislation, regulation, delegation or policy framework for the collection of information assets on behalf of the University. Within the University, the owner will typically be a Corporate Executive Portfolio Steward/ Principal Activity Steward/System Sponsor. Information owners define the policy which governs the information assets. An owner will often delegate the operational responsibility for information assets to a custodian, who applies controls that reflect the owner's expectations and instructions such as ensuring proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility of the information assets.
Physical Security	Provide physical protection of resources against deliberate or accidental threats, as well as from various forms of intrusion.
Principal Manager	Refer to 'Owner'. Includes any person authorised by the holder of that role to fulfil the duties and responsibilities of the role. The holder of the role, however, remains ultimately responsible for the correct and complete fulfilment of any delegated duties and responsibilities.
Public Information	Information that is already known or that can be provided to the public.
Resource	Refer to ICT Facilities and Devices and ICT Resources .
Resource Administrator. Resource Manager	A member of University staff who is delegated responsibility by the 'owner' for the effective, efficient and secure maintenance and operation of a University resource.
Responsibility	Ensuring that controls are in place so that clients of the University's ICT Resources and systems are not able to adversely affect other clients, resources, or systems.
Risk	The probability that a particular security threat will exploit a particular system vulnerability.
Risk Assessment	An evaluation of system assets and their vulnerabilities to threats, including potential losses that may result from threats.
Secure Information	Restricted information generally not released to all employees, and is not released outside of the organisation.
Security Incident (breach)	Any event that has, or could have, resulted in loss or damage to University assets, or an action that is in breach of the University security procedures.
Sensitive Information	Information that is releasable to all employees or to organisations associated with the University.

Separation of Duties	A security principle that assigns tasks which may affect the security of an information resource to several distinct individuals. Each user should have the least amount of privilege needed to perform those tasks.
Standard Operating Environment (SOE)	A common set of specific product and version types to be used on desktop systems across all University computers. Separate distinct SOE sets may apply to the administrative desktop environment and the academic desktop environment.
The University	The University of Southern Queensland.
Third Party	An individual or an organization outside of the University that provides labour or services.
User	Refer to Client
USQ	University of Southern Queensland.
Vulnerability	A weakness in the security system that might be exploited to cause loss or harm, either accidentally or deliberately by either internal or external entities.

2 Related Documents

Document (Electronic)	
Document (Hardcopy)	