Information and Communication Technologies Security Policy

INTRODUCTION

The University is committed to the appropriate use of Information and Communication Technology (ICT) and Services in support of its teaching, research, administrative and service functions. The University acknowledges an obligation to ensure appropriate security for all Information and Communication Technology data, equipment, and processes in its domain of ownership and control. Every member of the University shares this obligation, to varying degrees.

The University routinely gathers, stores, maintains, processes, transmits and disposes of records containing information. That information plays a vital role in supporting the University's business processes and customer services, in contributing to operational and strategic business decisions, and in conforming to legal and statutory requirements. Accordingly, information must be protected to a level commensurate with its value to the organisation, while still being made available to those who need it.

The University recognises that successful implementation of ICT security relies on having well informed Users combined with effective management procedures.

All Users should be aware of this policy, their responsibilities and legal obligations. All Users are required to comply with this policy and are bound by law to observe applicable statutory legislation.

STATEMENT OF AUTHORITY

The authority behind this policy is the *Charles Darwin University Act 2003* part 3, section 15.

COMPLIANCE

This is a compliance requirement under the *Charles Darwin University Act 2003* part 8, section 33.

INTENT

To provide definitive instruction on the safeguarding of personal and proprietary information and thereby protect the University from the adverse impact on its reputation and operations of failures of confidentiality, integrity and availability.

To ensure that Information and Communication Technology (ICT) facilities under the direction and control of Information Technology Management and Support (ITMS) - services, programs and data - are protected from threats, whether internal or external, accidental or deliberate.

This policy is applicable to:

- All staff members and students;
- All University Associates;
- All information assets encompassing facilities, data, software, paper documents and personnel;
- All clients of ICT equipment owned or leased by the University; and

- All equipment connected to the University data and voice networks.

RELEVANT DEFINITIONS

In the context of this document

Availability means the capacity of information systems:

- To be accessible and useable when required; and
- To be able to resist attacks and recover from failures;

Confidentiality means the principle of protecting information and preventing its disclosure to anybody other than those who have a right to access it and need to know;

Governance document means a formally approved document that outlines non-discretionary governing principles and intentions, in order to guide University practice. Governance documents are formal statements of intent that mandate principles or standards that apply to the University's governance or operations or to the practice and conduct of its staff members and students they include the Charles Darwin University Act (2003), by-laws, policies, procedures, guidelines, rules, codes and the Enterprise Agreement;;

Grey-Listing means a method of defending email users against spam. A mail transfer agent (MTA) using greylisting will "temporarily reject" any email from a sender it does not recognize. If the mail is legitimate the originating server will, after a delay, try again and, if sufficient time has elapsed, the email will be accepted. If the mail is from a spam sender, sending to many thousands of email addresses, it will usually not be retried;

Integrity means a standard of performance that guarantees information is created, amended or deleted only by the intended authorised means;

ICT facilities means Information and Communication Technology facilities operated by the University, whether owned or leased;

ITIL means Information Technology Infrastructure Library and is a set of best-practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of the business;

ITMS means the University's Office of Information Technology Management and Support;

ICT system means a related set of hardware and software used for the communication, processing and storage of information, and the electronic form of the information that they hold or process. This definition includes, but is not limited to, computers and their peripherals and other communication equipment, communication networks and other telecommunication facilities used to link such equipment together, and the operating software used on all such equipment;

Phishing means a way of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication;

RAID means Redundant Array of Independent Disks (originally Redundant Array of Inexpensive Disks), and is a storage technology that provides increased reliability and functions through redundancy. This is achieved by combining multiple disk drive components into a logical unit, where data is distributed across the drives in one of several ways called "RAID levels";

SaaS means Software as a Service and is a software delivery model in which software and its associated data are hosted centrally (typically in the (Internet) cloud) and are typically accessed by users using a thin client, normally using a web browser over the Internet. SaaS has become a common delivery model for most business applications, including accounting, collaboration, customer relationship management (CRM), enterprise resource planning (ERP), invoicing, human resource management (HRM), content management (CM) and service desk management;

Spam also known as Unsolicited Bulk Email (UBE), junk mail, or Unsolicited Commercial Email (UCE), means the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients; and

User means any person using any of the University's Information and Communication Technology facilities.

POLICY

Information and Communication Technologies security is concerned with ensuring the integrity and availability of information and services and maintaining the confidentiality of information. It is concerned with risk management and ensuring that internal controls are proportionate to risk. The University recognises the importance of ICT security. It is committed to ensuring all business activities performed with the use of ICT are protected and maintained, and that sustainable procedures are in place to reflect best practice ICT security.

IT security can be defined as 'the state of being free from or mitigating unacceptable risk'. The identified risks to the University concern the following categories of losses:

- Confidentiality of information - the privacy of personal or corporate information;
- Integrity of data - the accuracy and completeness of data. Protection is required against deliberate or accidental corruption of data;
- Assets - identifying and account for assets;
- Efficient and appropriate use - ensuring that University ICT resources and systems are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others; and
- System availability - concerned with the full functioning of a system and its components.

The potential causes of these losses are termed 'threats'. These threats may be human or non-human, natural, accidental, or deliberate.

The ICT Security Policy will deal with the following domains of security:

- Computer system security - Processor, peripherals, operating systems and applications. This includes information security;
- Physical security - Premises occupied by ITMS personnel and equipment or used for data storage;
- Operational security - Environment control, power equipment, and operational activities;
- Procedural security - By ITMS staff, vendor staff, management personnel, as well as staff and student Users; and
- Communications security - Communications equipment, personnel, transmission paths, and physical infrastructure.

Security Advisory Group

On a monthly basis ITMS will convene the Security Advisory Group. This group will consider security issues or proposed changes impacting the University's ICT security including services being provided by external

vendors or as SaaS, cloud or hosted solutions. Any proposals or recommendations put forward by this group must pass the Change Advisory Board prior to implementation. Critical issues will be escalated to the ICT Governance Committee or the University Executive as appropriate.

Access to Information and Communication Technologies Systems

All individuals who require access to ICT system and information resources will be properly identified, by means of a unique personal identifier.

Appropriate access controls will be introduced into every ICT system, with three objectives in mind:

- Preventing unauthorised Users from accessing and misusing the system;
- Constraining the authorised Users to their legitimate purposes; and
- To provide the ability to create audit logs detailing User's activity.

Automated procedures are enacted to define how additions, deletions, and other modifications to User access and privileges take place; this is handled by the University Identity Management (IDM) system which enforces the business rules for system access including requiring an authorising agent for each request.

The Identity Management system relies on the accuracy of the systems designated as 'sources of truth', these are:

- Alesco (CDU Staff Identities);
- Callista (CDU Student Identities);
- POSM (Non-CDU Student Identities); and
- MPOSTER (Non-CDU Staff Identities).

Exceptions are handled via a manual application process and require authorisation.

Authorised Users of ICT systems must:

- Be aware of his/her responsibilities and what he/she is authorised to do;
- Have an expectation of detection if he/she abuses that privilege; and
- Actively remove access privilege/s as soon as it is no longer needed or authorised.

For information on User responsibilities refer to the University *ICT Acceptable Use Policy* and *Email Acceptable Use Policy* and other associated governing documents.

Inactivity period

If there has been a period of inactivity on a desktop computer or terminal, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the User has provided the proper authentication. When sensitive systems are resident on desktop computers, authentication will also be required when the computer is powered on or restarted. All corporate applications will incorporate automatic time-out of log-ins after an appropriate period of inactivity.

Protection against malicious software

ITMS is responsible for procuring and facilitating the distribution of anti-virus software throughout the University within the Managed Operating Environment (MOE) and within the server space as appropriate.

Users with non-standard systems or systems that are not managed by ITMS are responsible for ensuring that virus checking and eradication takes place on systems for which they are the custodian.
To decrease the risk of the action of malicious software and to limit its spread:

- All software, data and attachments must be checked where practicable for viruses before installation;
- The provided software tools must be used to detect and remove viruses; and
- Systems that are shown to be infected will be isolated as quickly as practicable and until removal of the malicious software takes place.

Software licences

The University and all Users are personally responsible for complying with the Commonwealth *Copyright Act* and with the terms and conditions of the particular contracts or software licences relating to purchased, leased or acquired hardware and software. In particular, copying software without authorisation from the copyright holder is a breach of the Act.

ITMS is responsible for compliance and licensing for centrally managed software and packages.

Email

Spam is a serious issue as University ICT systems may be compromised resulting in the University becoming a source of spam. This may occur due to:

- A University host being infected with malware; or
- University credentials being used such that one of our mail servers becomes the source of spam.

In the first case, a virus or Trojan infects a client personal computer (PC) and hackers use that host to send spam. Often when this happens, the University's client PCs are part of what is called a botnet, a large collection of compromised PCs located across the world, all controlled by a central source. When this happens the University needs to remove/isolate the compromised PC from the network and clean the computer either by removing the malware or reinstalling the operating system and all software.

In the second, more serious case, University credentials obtained via a phishing attack or other method are used by hackers who connect to our mail servers and then generate a large volume of Spam. Spam is a significant problem on the internet and many organisations block email from IP addresses known to be the source of Spam. When the University's own mail servers start sending Spam our mail servers become blacklisted and our own legitimate email can no longer get through to many external organisations.

For the above reasons ITMS monitors all email looking for patterns that indicate that a high volume of spam-like email is being sent. When this happens a procedure is enacted to disable the compromised account, clear out any backlog of 'still to be sent spam' and then changes the internet protocol (IP) addresses of our mail servers to avoid mail being blocked by sites blacklisting the original mail server IP addresses.

As preventative measures ITMS runs scans on all incoming mail in an attempt to block malign or malformed mail packets from being received by the clients. This coupled with 'grey-listing' reduces both infected emails and the bulk of the unsolicited mail.

Acceptable Use

The University's policy on acceptable use of the ICT is contained in the *ICT Acceptable Use Policy* which defines the appropriate use of ICT resources. Users are required to read and agree to abide by this policy and associated procedures.
If, as an agent/representative of the University, the User has been granted access to external systems, the User agrees to abide by the rules of the remote site.

Data Integrity

ITMS is responsible for all sensitive, valuable, or critical information resident on the University's central storage systems. Data maintained on client PCs and laptops is the responsibility of the system user. ITMS does NOT backup locally stored data on workstations.

Centrally managed data must reside on RAID enabled storage on a Storage Area Network (SAN). Individual servers and datasets are periodically backed-up according to a defined schedule determined by the Tier (level) of the system in question.

An appropriate regular back-up schedule will be implemented to protect all data and software. A sufficient number of backups of all data and software will be stored off-site to protect against major damage occurring at the primary location.

Disaster Recovery and Business Continuity Planning

Adequate measures will be in place to prepare for and cope with disaster and to facilitate the resumption of business services in the event of a disruption and to minimise threats to the University's information assets.

All centrally managed data is mirrored to the University's Disaster Recovery (DR) site located at the Palmerston Campus, this includes the server cloud, application spaces and raw data volumes.

The system custodian is responsible for ensuring a Business Continuity Plan (BCP) is implemented for each system on the basis of sound risk assessment. Each BCP will be documented and provided to ITMS for consideration in its DR plan.

Change Management

Change control procedures through ITIL/ICT will provide a formal approach to the management of change enabling individual changes to be applied in a controlled and consistent manner.

A change control process must be used to ensure that all software, hardware, communications links and procedures move into production only after receiving proper authorisation from the Change Advisory Board (CAB).

The CAB will meet weekly to consider proposed changes, review enacted changes and provide analysis of failed or unsuccessful changes. The membership of CAB is flexible allowing for the participation of system owners external to ITMS.

Authority for Monitoring Activity

Users have a legitimate expectation to privacy in the carrying out of approved University activities. However, the University also has a right to inspect any data on a computer system connected to the University's resources (regardless of data or system custodianship), to prevent, detect or minimise

unacceptable behaviour on that computer system, and to provide to any authorised member of the University community, or law enforcement bodies, any information it possesses regarding the use of the University's resources. Where such action is taken, Users who have data inspected, and are found to be conforming to this policy, have a legitimate expectation that confidentiality will be preserved.

As part of the ICT security procedures, access to ICT systems must be monitored on a continuing basis and audit trails or access logs maintained of this access. This is carried out by ITMS.

The Director, ITMS will authorise specified staff whose duties include monitoring the use of ICT facilities or to investigate suspected security breaches or unauthorised access according to the process ratified under the *ICT Acceptable Use Policy*.

Physical Security

Physical security of ICT facilities is necessary to prevent unauthorised use and to ensure that systems are adequately protected against natural hazards, theft and damage.

Access to every office, computer room, and work area containing sensitive information, or the means to access such information, will be physically restricted.

Rooms and facilities, which house non-public ICT resources will be protected with physical security measures that prevent unauthorised persons from gaining access.

Training

To assist Users to gain an understanding of how ICT system security can be maintained and enhanced it is necessary to:

- Define security policies and procedures;
- Provide education and appropriate supervision; and
- Ensure an understanding of confidentiality requirements.

All aspects of ICT security will be incorporated into formal staff induction procedures for all new staff members and be conveyed to existing staff members on a regular basis. Similar training for students will occur when they first enrol at the University.

Periodic Management Review

Regular auditing procedures will be carried out on all computer systems to check for conformance to this policy, and to satisfy the requirements of the University's internal and external auditors. The depth and regularity of each level of audit should be outlined in the system procedures manual.

ITMS will periodically review the adequacy of information system controls as well as compliance with such controls.

ITMS are also responsible for the maintenance of the security measures documented in each system's security plan, and will conduct regular checks to ensure that the measures are being followed.

Policy Violation

A Formal Incident Response will be followed in the event of any breaches of security with the view to providing appropriate outcomes based on the risk and/or impact.

Action to correct and recover from security breaches will be defined so that:

- Only authorised Users are allowed access to ICT systems and data;
- All emergency actions taken are documented in detail;
- Emergency action is reported to management; and
- The integrity of business systems and security controls is confirmed with minimal delay.

All Users will be made aware of the procedures for reporting an incident and be required to report any observed or suspected incidents as quickly as possible to the correct authority. A formal reporting procedure will be established together with an incident response procedure (For further information refer to the *Identifying Unacceptable Use of Information and Communication Technologies Procedures* and the *Handling Suspected Cases of Unacceptable Use of Information and Communication Technologies Procedures*).

If a security breach involves facilities strictly internal to the University, the appropriate University disciplinary procedures will be followed. In the case of serious breaches of this policy by staff, disciplinary procedures for 'misconduct' or 'serious misconduct' may lead to sanctions being imposed; including termination of employment [refer to the ICT Acceptable Use Policy and the CDU and Union Enterprise Agreement]. In the case of students appropriate action with be taken in accordance with the CDU Student Conduct By-Laws.
The University will refer any incident involving a possible breach of Territory, Commonwealth or International law to the appropriate authority for investigation. The University will give that authority all reasonable assistance.

If a security breach occurs in which a person or organisation external to the University is involved as a potential victim of the breach, the University will refer to the external party, the details specific to that party.

Procedures will be established by ITMS, documented and maintained for establishing the cause of any security breach, whether accidental or deliberate, the corrective action to be taken, and any recommendations on preventing a recurrence. Internal controls will monitor the implementation and effectiveness of any corrective action, including any required changes to existing procedures.

ESSENTIAL **SUPPORTING** INFORMATION

Internal

Charles Darwin University and Union Enterprise Agreement 2013

Email Acceptable Use Policy

Information and Communication Technologies Acceptable Use Policy

Handling Suspected Cases of Unacceptable Use of Information and Communication Technologies Procedures

Identifying Unacceptable Use of Information and Communication Technologies Procedures

Information Privacy Policy

Student Conduct By-laws

External

Copyright Act 1968 (Commonwealth)

Information Act 2002 (NT)

Information Regulations 2010 (NT)

Privacy Act 1988 (Commonwealth)

Spam Act 2003 (Commonwealth)

Surveillance Devices Act 2007 (NT)

Surveillance Devices Regulations 2010 (NT)

Telecommunications (Interception and Access) Act 1979 (Commonwealth)

Document History and Version Control

Last amendment:	15 Dec 2017	**Next Review:**	Mar 2018
Sponsor:	Deputy Vice-Chancellor, Operations		
Contact Officer:	Director, Information Technology Management and Support		

Version	Date Approved	Approved by	Brief Description
1.00	9 Nov 2011	Vice-Chancellor	Creation of original document and upload to CDU website.
1.01	10 Jan 2012	Governance	• Update hyperlinks • Minor changes to grammar and formatting
1.02	11 Feb 2013	Governance	• Convert document to new template • Updated and added hyperlinks • Minor changes to wording, formatting and grammar • Assigned document number • Changed IT to ICT in line with other governing documents • Added relevant definitions
2.00	25 Mar 2015	Governance	There were no suggested changes to this policy by the ICTG Committee on 19 Feb 2015. The Committee agreed the policy had been useful and recommended it be submitted to Governance for acceptance and use in its current format. • Governance updated the template, minor grammatical amendments and updated the hyperlink to the Information Privacy Policy
2.01	15 Dec 2017	Governance	• Conversion to new Governance template due to new University branding • Updated definitions • Updated hyperlinks • Amended Sponsor from VC to DVC, Operations • Replaced shall with will