INFORMATION SECURITY POLICY					
Policy Group(s):					
Type:	Policy		Guideline		
	Procedure		Regulation		
CPUT Statute and/or Regulation Reference No and date:					
Relevant Legislation and/or policy, Codes of practice, Professional Authorities:	• Electronic Communications and Transactions Act, • Promotion of Access to Information Act, • King Report on Corporate Governance for South Africa - 2002 (King II Report). Now being superseded by the King III Report.				
Relevant Institutional policies/ Documents/manuals/ Handbooks	• Electronic Communication Policy				
Policy Reference and Version No:					
Certification of Due process:	_____ Vice Chancellor		_____ Date		
Approval Date	April, 2009	**Commencement Date**	April, 2009	**Review Date**	April, 2012

Key Words for Search Engine:	Information Security Policy, ECT Act, Compliance, Data classification, Confidentiality, Password management, Logical Security, Physical Security

REVISION HISTORY:				
Revision Ref No.	**Approved/ Rescinded**	**Date**	**Authority**	**Resolution Number or Minutes Reference**
1.0				

POLICY STATEMENT	
1.0 Intent	The purpose of this policy is to ensure that due care is exercised in protecting the information systems and data of Cape Peninsula University of Technology (CPUT)
2.0 Scope	2.1 CPUT has a large store of information, ranging from administrative information such as salaries, accounts and examination results to proprietary information such as information produced by the students and lecturers. 2.2 As in any educational institution, the sharing of information, gathering of information and interpreting of information forms the basis of the institution. It

	is for this reason that an information security policy needs to strike a balance between protecting its core resource, information, and enhancing learning through the sharing of information. 2.3 The security of information is of paramount importance to the ongoing confidentiality, integrity and availability of CPUT's information systems and to deriving the maximum return on its investment in Information and Communication Technology (ICT). CPUT is continually upgrading and investing in its ICT Infrastructure. This CPUT Information Security Policy applies to: 2.3.1 All CPUT Staff and students, including temporary workers, and independent contractors working for or on the premises of CPUT all electronic information, including: 2.3.1.1 Data processed and stored on line, e.g. information on the network, or personal hard drives; 2.3.1.2 Backed up data; 2.3.1.3 Archived data, or other off line storage, such as laptops; 2.3.1.4 Audit logs; 2.3.1.5 Data stored on compact discs (CDs) or floppy disks; 2.3.1.6 e-mail; 2.3.1.7 Information printed from CPUT information systems; 2.3.1.8 Information in all stages of its life-cycle, from creation through entry, processing, communication, dissemination and storage, to disposal. 2.4 All information travelling over CPUT computer networks that has not been specifically identified as the property of other parties will be treated as though it is a CPUT asset. 2.5 The successful implementation of this policy is a necessary step for CPUT to adhere to the relevant Acts of Parliament, as well as to abide by the recommendations of the King II Report. 2.6 The following principles, standards and procedures have been established to formalise the information security process at CPUT.
3.0 Objective(s)	The objectives of this policy are to: • Provide direction as to what CPUT wants to achieve regarding information security. • Promote awareness amongst all staff (academic and administrative), students, contactors and consultants of the value of information and the risks involved in working with or handling information.

	• Provide for the necessary protection of information, thereby ensuring its confidentiality, integrity and availability.
4.0 Definitions and Acronyms	**4.1 DUE CARE** is defined as the cost-effective protection of information at a level appropriate to its value. The value of the information can be quantified as the risk to CPUT if the information should be lost or compromised. **4.2 CPUT'S INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) INFRASTRUCTURE** is defined as the network, including Local Area Network (LAN) and Wide Area Network (WAN); and peripherals controlled and maintained by CPUT's Computer and Telecommunications Services (CTS) Department. **4.3 A STAND-ALONE SYSTEM** is any computer not connected to CPUT's ICT infrastructure. **4.4 A DATA CUSTODIAN** of an area of the institution's data is that member of the CPUT Executive Committee having management responsibility for the Data Managers, Data Owners and Data Users in that area. **4.5 A DATA MANAGER** is a line manager to whom one or more Data Owners report. **4.6 A DATA OWNER** is a senior Data User, with assigned responsibility for the correct functioning of a sub-system. **4.7 A DATA USER** (or User) is an employee (permanent or temporary) who interacts with a CPUT database, with authority to read, enter, update or delete information. **4.8 A SYSTEM ADMINISTRATOR** is the person/s responsible for maintaining the supporting infrastructure, servers and access controls, including database administration and system ownership. **4.9 AN INFORMATION SECURITY OFFICER** is a member of the CTS Department with responsibility for information security issues. **4.10 A DOCUMENTATION CONTROL OFFICER** is a member of the CTS Department with responsibility for the management of documentation within the department. **4.11 A SOFTWARE DEVELOPER** is anyone who develops or revises any software used by CPUT, whether employed by CPUT or contracted by CPUT for the purpose. **4.12 ON-SITE** is defined as any area of work within the general operational area of CPUT. This includes the remote campuses. **4.13 OFF-SITE** is defined as any residential home or property, and any location outside the general operational area.

4.14 BUSINESS DATA is defined as any data required for the completion of daily tasks and duties. This includes Microsoft Excel spreadsheets and Microsoft Word documents.

4.15 SANITISED DATA is production information that no longer contains specific details that might be restricted or confidential. This data is typically used for testing and training purposes.

4.16 The classification of information is a key element in the protection of information against unauthorised disclosure. Unauthorised disclosure occurs when sensitive information finds its way into the hands of staff, students or others who should not have access to this information. The purpose of an information classification system is to:

4.16.1 Promote awareness amongst all CPUT management, students and staff of the need to protect information against unauthorised disclosure;

4.16.2 Provide a framework for establishing the level of protection required to ensure that information is adequately protected when it is being processed or handled.

Data is classified according to the following classes:

Information Class	Description
Restricted	Highly sensitive information, disclosed only to persons specifically authorised by name, e.g. information regarding pre-released exam results.
Confidential	Sensitive information disclosed only to those with an identified need to know the information. The information is normally defined in terms of groups rather than by individual names. This also refers to any sensitive information provided to CPUT by external organisations.
Internal	Information that is not sensitive but is not intended for release to the general public. When directed by CPUT management, some internal information may be subject to limited release to specific external entities. Generally, internal information should be available to all CPUT staff, e.g. policy documents, management information.
Copyright / Patent	Information that is the property of CPUT and should not be copied by external parties, but is intended for release to the general public and external parties, e.g. student papers and projects.
Public	Information, such as student projects, that is specifically intended for release to the general public.

5.0 Policy/ Procedure Principles	**5.1 POLICY PRINCIPLES** **5.1.1 Information Security has three dimensions:** **5.1.1.1 Confidentiality** (the sensitivity of the information to unauthorised disclosure); **5.1.1.2 Integrity** (the accuracy of information and the authenticity of transactions); and **5.1.1.3 Availability** (the need to have access to the information on demand). This policy addresses all three of the dimensions. **5.1.2 The following Information Security principles relate to one or more of these dimensions.** 5.1.2.1. User Identification and Authentication • Every user and third party requiring access to the CPUT ICT infrastructure and stand-alone systems must have a unique user ID and a personal secret password. This user ID and password will be required to establish positive identification and authentication. • Users are accountable for all activities performed with their personal user IDs. User IDs may not be used by anyone other than the individuals to whom they have been issued. • All users are to comply with the CPUT Security Policy. Non-compliance will result in disciplinary action, according to the nature and severity of the transgression. • All computers that connect to the CPUT ICT infrastructure must make use of proper password access controls that prohibit access to resources without proper authentication procedures. • Every authentication process for computers connecting to the CPUT ICT infrastructure must include a notice warning against unauthorised use and the consequences thereof. • The CTS Department is responsible for continuously making users aware of the acceptable use of user ID's and passwords 5.1.2.2. Safeguarding of Information Assets and Resources • All ICT assets and resources are the property of CPUT. • Cost-effective safeguards or controls need to be implemented to adequately protect ICT assets and resources from loss, misuse, disclosure or modification. • The level of security afforded to ICT assets and resources is determined by their value, sensitivity and importance to CPUT. • Access to the CPUT ICT infrastructure and stand-alone systems is not open and is granted to approved users on the basis of positive identification and authority. • Each data type (Financial, Examination Results, etc.) will have a designated Data Manager, who will be responsible for the management of that data. The Data Manager will determine users' type and level of access to data.

- The boundaries of data management will be agreed upon between the Data Managers, the Data Quality Committee, and the Data Custodians.
- All administrator-equivalent user IDs and passwords are to be known only to the individuals responsible for the administration of the CPUT ICT infrastructure, applications and databases. These are to be written down and sealed in an envelope, which is to be locked in the safe of the Director of CTS. The Information Security Officer must co-ordinate this task. This information is to be accessed in emergencies only i.e. when the System Administrator is unavailable. The user IDs and passwords are to be changed immediately thereafter.
- Access to applications is to be granted by the CTS Department, on the authority of the relevant Data Manager.
- The Human Resources and Registration Departments are to provide the CTS Department with up-to-date and relevant staff and student details to permit the implementation of appropriate security controls . In particular, staff who have left the employ of CPUT and students who are no longer registered should have all access rights and privileges revoked.
- Heads of Department are responsible for all information assets and resources in their department. CPUT's ICT infrastructure is owned by the CTS Department.
- Where individuals are visiting the institution, they must abide by the existing security practices. In particular equipment brought onto the site, which has to be linked to the institution's infrastructure, will have to undergo the relevant scrutiny by the technical staff of the CTS Department.

5.1.2.3. Availability

- All procedures designed to minimise the risk of data loss through computer virus infections must be strictly adhered to in order to ensure the availability of CPUT's ICT Infrastructure.
- All data located on the ICT infrastructure and other systems, which is the responsibility of the CTS Department, is to be backed up. Users are responsible for backing up data located on their computers. In addition and in line with the relevant legislation, the CTS Department must ensure that email content is adequately archived.
- All breaches of security are to be reported to the Director CTS as soon as possible and handled according to defined procedures. The Information Security Officer will then process the matter.
- All ICT assets and resources are to be maintained in accordance with the manufacturer's requirements, to maximize the lifespan of assets and resources.
- Where possible, the use of redundant solutions is to be used. Redundancy of systems ensures continued availability. Redundancy must be a key element for all core systems.

5.1.2.4. Systems Development and Maintenance

- Before a new system is acquired or implemented, Heads of Department, Data Managers or Data Owners must consult with the

	Director of CTS in order to specify the security requirements. Alternatives must be reviewed with the vendors and implementation consultants so that an appropriate balance is struck between security and other objectives (ease-of-use, operational simplicity, ability to upgrade, acceptable cost, etc.). • All software testing and training for systems must be accomplished exclusively with sanitised test data provided by the Data Owners. All testing must take place on a proper test environment. • All application development must take place on a test environment. This is the responsibility of the Software Developer. • Software Developers must ensure that all developed software follows a sign-off procedure. • New application software still in the development and testing phase must be kept strictly separate from live application software. If existing facilities permit it, this separation must be achieved via physically separate computer systems. 5.1.2.5. System Change Control • The change control process must not compromise the existing security of the CPUT ICT infrastructure and stand-alone systems. • All changes to systems must be documented, tested and approved in a controlled and systematic manner before implementation. • All intermediate and final products of the systems development process either purchased or developed at the direction of CPUT are the exclusive property of CPUT and are solely for CPUT's use. • CPUT management must ensure that all development and maintenance activities (hardware, software and infrastructure) performed by both external companies and in-house, subscribe to CPUT's change control principles, standards and procedures. 5.1.2.6. Auditing, Logging and Monitoring • CPUT's ICT infrastructure and other systems must be monitored by the CTS Department on an on-going basis for security violations and suspicious activity. • Any security breaches detected by the standard auditing, logging and monitoring tools will be addressed by the CTS Department within 16 working hours. An investigation will be launched by the Director CTS should this time period be exceeded. • CPUT reserves the right to monitor all traffic on the CPUT network in accordance with the relevant legislation and the Electronic Communications Policy. • The CTS Department must ensure that annual ICT audits are completed and that the findings of the audit report are appropriately actioned. 5.1.2.7. Documentation • Documentation related to the ICT infrastructure must be readily available and kept up-to-date. • The control of the documentation process is the responsibility of the Documentation Control Officer.

	• It is necessary to enforce this Information Security Policy in order to protect CPUT's legal rights. Any staff member, student or contractor who does not comply with the spirit and intent of this policy and its supporting standards will be subject to appropriate disciplinary action. This may include: revoking of access privileges, termination of agreements or contracts, or dismissal. Security breaches must be reported to the Director of CTS as soon as the breach is suspected or becomes known, whether directly or via a Data Manager or Data Owner.
6.0 Responsibility	**6.1 RESPONSIBILITIES** 6.1.1 The responsibilities of CPUT's Executive Management, as **Data Custodians,** include: 6.1.1.1 Accepting accountability for the information assets under their control 6.1.1.2 Exercising a fiduciary duty to properly protect CPUT's information assets from a variety of threats such as error, fraud, embezzlement, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption, system failure, and disaster 6.1.1.3 Providing the appropriate resources, both personnel and financial, for information asset protection and risk management 6.1.1.4 Responding to identified exposures and vulnerabilities 6.1.1.5 Supporting the investigation and resolution of information-related losses and incidents 6.1.1.6 Ensuring the implementation of CPUT's Information Security Policy. 6.1.2 The responsibilities of the **Data Managers** include: 6.1.2.1. Accepting accountability for the quality of data in the sub-systems under his or her authority 6.1.2.2 Establishing or implementing policies and procedures for data capture and usage, where appropriate 6.1.2.3 Assigning an appropriate Data Owner for each of the sub-systems 6.1.2.4 Ensuring that all Data Users are properly trained 6.1.2.5 Specifying and communicating the security requirements of the system 6.1.2.6 Authorising access to CPUT's administrative data systems 6.1.2.7 Liaising with the CTS Department for additional functionality, where

	necessary 6.1.2.8 Handling day-to-day security lapses and reporting security breaches to the Director: CTS 6.1.2.9 Ensuring that all Data Owners and Data Users in his or her section are aware of the contents of this policy. 6.1.3 The responsibilities of the **Data Owners** include: 6.1.3.1 Accepting accountability for the integrity of the data in a sub-system 6.1.3.2 Ensuring that the policies and procedures set by the Data Manager are adhered to 6.1.3.3 Administering the access and other controls specified by the Data Manager 6.1.3.4 Liaising with the CTS Department for additional training, fault logging, and functionality required within the sub-system 6.1.3.5 Running data validations, assigning Data Users to correct the validation errors, and following up on the validations 6.1.3.6 Reporting any security breaches to the Data Manager or the Director: CTS 6.1.4 The responsibilities of the **Data Users** include: 6.1.4.1 Accessing only those information systems and data to which they are specifically authorised 6.1.4.2 Using the information only for the purpose intended by the University 6.1.4.3 Complying with all security measures established 6.1.4.4 Reporting security breaches to the Data Owner or the Director: CTS 6.1.4.5 Not disclosing confidential information to anyone without proper authority, as defined in applicable CPUT policies or procedures 6.1.4.6 Abiding by the provisions of this policy 6.1.4.7 Accepting accountability for the quality of the data which he or she handles, in terms of accuracy, completeness, and timeliness 6.1.4.8 Cleaning up data validations as assigned by the Data Owner or Data Manager 6.1.5 The responsibilities of the **System Administrator** include:

	6.1.5.1 Ensuring that appropriate virus protection and detection measures and controls are in place throughout CPUT 6.1.5.2 Monitoring network activity for potential security breaches 6.1.6 The responsibilities of the ***Director of CTS*** include: 6.1.6.1 Acting as the custodian of this policy 6.1.6.2 Providing the infrastructure for the various computer related operations 6.1.6.3 Protecting the integrity of the systems 6.1.6.4 Providing support in planning, implementing and administering information security 6.1.7 The responsibilities of the **Information Security Officer** include: 6.1.7.1 Co-ordinating information security within CPUT 6.1.7.2 Developing and maintaining this information security policy and supporting standards 6.1.7.3 Investigating security problems / breaches 6.1.7.4 Ensuring that staff, students and contractors to CPUT are properly educated and aware of this information security policy and its implications on an ongoing basis 6.1.8 The responsibilities of the **Documentation Control Officer** include: 6.1.8.1 Controlling access to all the documentation in the CTS Department 6.1.8.2 Managing the electronic and physical location of the documentation 6.1.8.3 Developing and maintaining the documentation processes and standards 6.1.8.4 Keeping track of documentation changes and versions 6.1.9 The responsibilities of all **Contractors** with access to electronic information include: 6.1.9.1 Ensuring awareness by their employees of the contents of this security policy and its implications 6.1.9.2 Accessing only those information systems and data specifically authorised regarding all CPUT information collected or accessed during their interaction with CPUT as *confidential* and, as such, not to use, disclose, transfer or

	amend any information gathered during their stay without the explicit consent of the information owners

7.0 Accountability and Authority:	
Implementation:	CTS and DATA Managers
Compliance:	CTS
Monitoring and Evaluation:	CTS and QMD
Development/Review:	CTS
Approval Authority:	Council
Interpretation and Advice:	CTS and QMD

8.0 Who should know this policy?
All staff, students and visitors who use the Electronic Systems at CPUT; All Software Developers who provide services to CPUT

9.0 Policy/procedure implementation plan	The standards and procedures listed below, maintained by the CTS Department, are supportive of this Information Security Policy. **9.1 User Identification and Authentication** Standards • CPUT Password Standards • Procedures User Password Management • Password Use • Changing your password **9.2. Safeguarding of Information Assets and Resources** Physical Security Procedures • Security of Computer Rooms • Environmental Security • Equipment Security on-site • Equipment Security off-site Logical Access Security Procedures • Request for Additional Privileges • Management of User Access • Application Access Control • Database Access Control Remote Access Procedures **9.3 Availability** Protection from Malicious Software (Viruses) – Procedures • Minimising the risk of a virus infection • Responding to a virus infection Data Backup Procedures • Server backups • Workstation backups Breaches of Security Procedures Maintenance of Equipment Procedures Redundancy Procedures

	9.4 Systems Development and Maintenance **9.5 System Change Control** Change Control Policy **9.6 Auditing, Logging and Monitoring Procedures** **9.7 Documentation Procedures** Documentation Control Policy
10.0 Resources required	A staff member in the CTS department, dedicated to the Information Security operation. The individual will organise regular information security forums and user awareness programmes. The active input of the Data Managers is key to the success of the implementation.

12.0 Answers to FAQ	
	1. Why is the Information Security Policy important? It is important that an institution sets out the principles for safeguarding its electronic assets. There is an added responsibility placed on institutions by the recommendations of the King II report in embrace good governance in areas such as Information Security

EFFECTIVENESS OF THE POLICY	
Performance Indicator(s):	Awareness Programmes Physical Access logs Logical Access logs Anti-virus deployments records Backup Records Change control effectiveness through activity monitoring