University of Cape Town Information Security Policy

Document summary

Effective date	May 2020	**Last updated**	24 February 2020
Document owner	Registrar University of Cape Town		
Approved by	UCT Council	**Reviewed by**	RMEC, UICTC and SEC
Enquiries	Director Enterprise Infrastructure Services		

Table of Contents

1. Purpose

The purpose of this information security policy is to:

1.1. ensure the safety of all UCT staff, students and persons reliant upon and/or who use UCT's information systems by protecting their personal identifiable information
1.2. ensure that all of UCT's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, and that this protection is cost-effective;
1.3. ensure that all users are aware of and fully comply with this policy statement and all associated policies, and are aware of and work in accordance with the relevant procedures and codes of practice;
1.4. ensure that paper records are kept securely and managed effectively;
1.5. ensure that all users are aware of and fully comply with the relevant South African legislation;
1.6. create across UCT an awareness that appropriate security measures must be implemented as part of the effective operation and support of information management systems;
1.7. ensure that all users understand their own responsibilities for protecting the confidentiality and integrity and availability of the information and data they handle;
1.8. ensure that information is archived or disposed of in an appropriately secure manner when it is no longer relevant or required.

2. Definitions Additional Information and Training

2.1. Definitions of the terms used in this policy statement and supporting documentation may be found in the Glossary of Terms.
2.2. Those requiring information, explanation or training about any aspects of the policy, which relate to computer security should discuss their needs with the Information and Communication Technology Services (ICTS): Enterprise Infrastructure Services (EIS): Information and Cyber Security Services Team (ICS). Questions about the creation, classification, retention and disposal of records (in all formats) should be directed to the Office of the Registrar. The Registrar and the Executive Director ICTS (EDICT) will in the first instance be responsible for the interpretation and clarification of the information security policy.

3. Glossary of Terms

Term	Definition
CSIRT	Computer Security Incident Response Team; Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents.
Cyber security	The ability to protect or defend the use of cyberspace from cyberattacks. (NIST, n.d.)
Data Steward	Senior level individuals appointed as Data Stewards for all sets of data. As a general principle, data will be stewarded by the head of the section that captures and/or collates the data.
EDICT	Executive Director Information and Communication Technology Services
Guidelines	Guidelines are recommendations where specific standards do not apply or exist
Information	"Information is an asset that, like other important business assets, is essential to an organisation's business and consequently needs to be suitably protected. Information can be stored in many forms, including:

	digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees." (ISO/IEC 27000:2018)
Information security management system	An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets. (ISO/IEC 27000:2018)
Information systems	A system for generating, sending, receiving, storing, displaying or otherwise processing data and/or data messages and includes the UCT network and the Internet
Institutional data	Any data that are owned and/or licensed by the University of Cape Town
ISWG	Information and Cyber security Working Group. A sub-committee of the Risk Management Executive Committee (RMEC)
Management and/or manager	Means, all levels of line management academic or PASS at UCT including, but not limited to; the Vice-chancellor, Deputy Vice-chancellors, Deans, Heads of Academic departments, Executive Directors and PASS line management
Policy	A formal statement produced and supported by senior management, which reflects UCT's desired objectives of its information security program and activities
Primary activity	Primary activities are teaching and learning, research and social responsiveness
Procedures	Procedures are detailed step by step instructions on how to achieve a given goal or mandate
TENET	Tertiary Education and Research Network of South Africa
RMEC	Risk Management Executive Committee
Secondary activity	Secondary activities are those activities that are in support of the primary activities and include, Administration, Finance, Human Resources, Information and Communication Technology Services, Properties and Services, UCT libraries and so forth
SANReN	South African National Research Network
Standards	Standards are mandatory statements or rules that are supportive of and provide direction for formal policies
UCT CSIRT	University of Cape Town Computer Security Incident Response Team, a function of the Information and Cyber security Team within the Enterprise Infrastructure Services Division of the Information and Communication Technology Services Department. Refer to CSIRT

4. Policy Statement

4.1. The university of Cape Town (UCT) is committed to engaging with the key issues of our natural and social worlds through outstanding teaching, research and scholarship, by necessity UCT focuses on exploiting information to achieve its mission.

4.2. Next to people, information is UCT's most important asset. The information we use exists in many forms: printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Regardless of the form it takes, or means by which it is shared or stored, information should always be protected appropriately.

4.3. Information security is characterised here as being concerned with guaranteeing availability (ensuring that authorised users always have access to information when they need it), integrity (safeguarding its accuracy and completeness), confidentiality (ensuring that sensitive information is accessible only to those authorized to use it), and authenticity. It must also address proper methods of disposal of information that is no longer required. Security is essential to the success of almost every academic and administrative activity. Effective security is achieved by working within a proper framework, in compliance with legislation and UCT's policies, and by adherence to approved procedures, codes of practice and grant/funding terms and conditions.

4.4. The UCT Council has approved this policy statement and delegated its implementation to UCT management

5. Applicable to

5.1. The policy applies to all staff and students of UCT and all other computer, network or information users authorised by UCT or any department or faculty thereof. It relates to their use of any UCT-owned facilities (and those leased by or rented or on loan to UCT), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the UCT network; to all UCT owned or licensed data and programs (wherever stored); and to all data and programs provided to UCT by sponsors or external agencies (wherever stored). The policy also relates to paper files and records created for the purposes of UCT business.

6. Framework

6.1. The University's information security is managed through the below Framework which comprises:
6.1.1. this Policy and sub-policies (Appendix A),
6.1.2.Standards,
6.1.3.Guidelines and
6.1.4.Procedures, alongside supporting Governance and management processes.

6.2. This Framework provides a flexible and effective platform upon which the University's information security objectives are met. The Framework is detailed below:

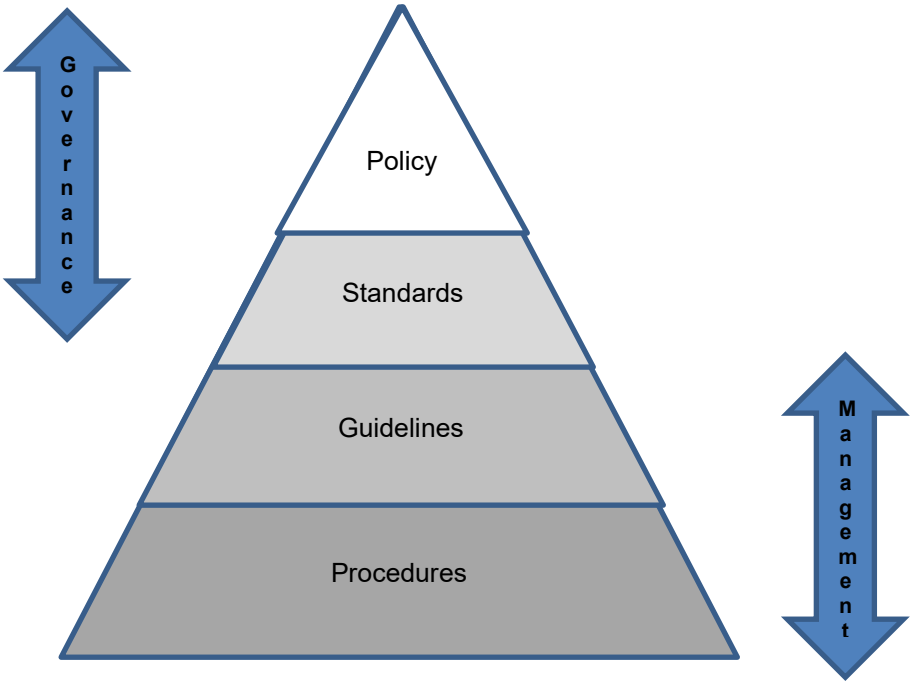

Fig 1 UCT Information and Cyber security Framework

6.3. This Policy can be met by adopting and complying with policy, sub-policy and associated standards. However, the Framework is designed to be flexible and allow a range of methods to meet this Policy. It enables local autonomy in how the outcomes and objectives of this Policy are met, by allowing local procedural methods and/or controls to be implemented. At the same time, it allows those who require further advice from the UCT CSIRT to meet this Policy through the methods detailed in the Procedures. Regardless of the approach, all within scope of the Policy are required to meet this Policy and the Standards using appropriate methods.

6.4. It is important to note that the Standards, as outlined in the associated documentation, must be considered the minimum requirements for information security (or the 'baseline'). Where additional information security controls are required for research, legal, regulatory or governance purposes, the controls must be enhanced accordingly. The Information and Cyber security Team in ICTS Enterprise Infrastructure Services Division can provide advice on how to comply with additional security requirements, where required.

7. Policy details

7.1. Responsibilities for Information and Cyber security

7.1.1. The UCT Council is accountable and responsible for defining an information security policy and for ensuring it is carried out by all academic and professional services departments and faculties through the respective manager. The policy will apply to associate bodies e.g. UCT owned companies and students' associations.

7.1.2. UCT executive and senior management shall establish at UCT, implement, maintain and continually improve an information security management system, in accordance with International Standards Organisation 27000 series standard, the requirements of this policy, demonstrate leadership and commitment with respect to the information security management system by:

7.1.2.1. ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organisation

7.1.2.2. ensuring the integration of the information security management system requirements into the organisation's processes

7.1.2.3. ensuring that the resources needed for the information security management system are available;

7.1.2.4. communicating the importance of effective information security management and of conforming to the information security management system requirements;

7.1.2.5. ensuring that the information security management system achieves its intended outcome(s);

7.1.2.6. directing and supporting persons to contribute to the effectiveness of the information security management system;

7.1.2.7. promoting continual improvement; and

7.1.2.8. supporting other relevant management roles to demonstrate their leadership as it applies to their areas

7.1.3. All who make use of UCT's systems and information have responsibility for protecting those assets. Individuals must, at all times, act in a responsible and professional way in this respect, and will refrain from any activity that may jeopardise security.

7.1.4. Managers are required to implement this policy in respect of both paper and electronic systems operated by their Faculties, Departments and are responsible for ensuring that staff, students and other persons authorised to use those systems are aware of and comply with it and associated codes of practice. Managers should ensure adequate oversight of security (in consultation with the UCT Computer Security Incident Response Team), through central and departmental IT support staff or otherwise.

7.1.5. The Information and Cyber security Working Group (ICWG) advises the Risk Management Executive Committee (RMEC) on matters related to compliance with this policy, and is responsible for regularly reviewing it for completeness, effectiveness and usability.

7.1.6. The ICWG will also arrange for analysis of security assessments received from departments, and report on these to the RMEC.

7.1.7. The Director EIS and the Senior Manager ICS, in addition to their involvement in policy making, provides relevant operational services. These include operating a Computer Security Incident Response Team, which provides incident response and coordination, dissemination of security information, training, consultancy, and liaison with other external security teams and law enforcement agencies.

7.1.8. It is the responsibility of each individual to ensure his/her understanding of and compliance with this policy and any associated procedures or codes of practice.

7.1.9. Staff with supervisory responsibility should make their supervised staff or students aware of best practice.

7.1.10. Staff and students who process or who are responsible for the processing of personal data, as defined in UCT's Data Protection Policy, are additionally required to understand and comply with all obligations placed upon them under agreements with external parties, including but not limited to information security, integrity and perpetual confidentiality.

7.2. Compliance with Legislation

7.2.1. UCT, each member of staff, and its students have an obligation to abide by all South African legislation. Of particular importance in this regard are;

- 7.2.1.1. Electronic Communications and Transactions Act 2002 as amended,
- 7.2.1.2. Protection of Personal Information Act 2013,
- 7.2.1.3. Promotion of Access to Information Act 2000,
- 7.2.1.4. Consumer Protection Act 2008,
- 7.2.1.5. Electronic Communications Act 2005,
- 7.2.1.6. Protection of Constitutional Democracy against Terrorist and Related Activities Act 2004,
- 7.2.1.7. the regulation of Interception of Communications and Provision of Communication-related Information Act 2008 and/or as amended and,
- 7.2.1.8. the Films and publications act 65 of 1996 and/or as amended

7.2.2. Of importance is Section 19 of the Protection of Personal Information Act 2013 which requires a responsible party to secure personal information through technical and organisational measures. The responsible party must identify reasonably foreseeable risks to personal information and effectively implement safeguards against these risks. Safeguards should be reviewed and updated in response to new risks or deficiencies in implementations.

7.2.3. Relevant legislation is referenced in supporting polices and guidelines. Full texts are available from the South African Government web site: https://www.gov.za/documents/acts

7.3. Risk Assessment and Security Review by Departments

7.3.1. Information and data should be suitably classified according to the guidance given in section 7.2 of this policy

7.3.2. Stewards should adopt a risk-based approach to assessing the value of information handled, its sensitivity, the potential damage or distress caused by a loss of the information and the appropriateness of technological, organisational and physical security controls in place or planned. Without proper assessment of the value of information assets, and the consequences (financial, reputational and otherwise) of loss of data or disruption to service, efforts to improve security are likely to be poorly targeted and ineffective.

7.3.3. Reviews should be conducted on an annual basis, to take into account changes to technology, legislation, business requirements and priorities and at the point of new data being assigned to the Data Steward. Security arrangements should be revised accordingly.

7.4. Information Security Incident Response

7.4.1. Information security incident response policy, plan and procedures shall be defined implemented, maintained, continually improved, taking into account; the International Standards Organisation's "*Principles of Incident handling*" ISO/IEC 27035-1 and particularly the "*Guidelines to plan and prepare for incident response*" ISO 27035-2.

7.5. Breaches of Security

7.5.1. Any individual suspecting that the security of a computer system has been, or is likely to be, breached should inform the UCT CSIRT immediately. UCT ICWG will advise UCT via RMEC on what steps should be taken to avoid incidents or minimize their impact, and identify action plans to reduce the likelihood of recurrence.

7.5.2. In the event of a suspected or actual breach of security, UCT CSIRT may after consulting the Director Enterprise Infrastructure Services or his/her designate, require that any unsafe systems, user/login names, data and/or programs be removed or made inaccessible.

7.5.3. Where a breach of security involving either electronic or paper records relates to personal data, the UCT CSIRT must be informed, as there may be an infringement of Protection of Personal Information Act 2013, which could lead to intervention by the Regulator and potentially civil or criminal proceedings. It is vital, therefore, that users of UCT's information systems comply, not only with this policy, but also with UCT's Data Protection Policy and associated codes of practice, details of which may be found on the UCT website.

7.5.4. All physical security breaches should be reported to Campus Protection Services and the UCT CSIRT.

7.5.5. ICTS and the UCT CSIRT may monitor network activity, receive reports from SANReN, TENET and other security agencies, and take action or make recommendations consistent with maintaining the security of UCT information assets.

7.6. Policy Awareness and Disciplinary Procedure

7.6.1. The contract of employment shall state that employees are required to comply with the Information Security Policies, including such additions or amendments thereto as may be made by UCT from time to time.

7.6.2. As part of an induction process, Managers are reminded to ensure that the inductee is directed to and is made aware of the content of this policy.

7.6.3. Students are required to comply with the Information Security Polices, including such additions or amendments thereto as may be made by UCT from time to time.

7.7. Supporting Policies, Procedures and Codes of Practice

7.7.1. Supporting policies, standards, guidelines, procedures and codes of practice amplifying this policy statement are published with it and are available on the UCT website. Staff, students, contractors and other third parties authorised to access the UCT network to use the systems and facilities identified in section 5.1 of this policy, are required to familiarize themselves with these and to work in accordance with them. Guidance notes will also be published to facilitate this.

7.7.2. Other agencies, such as National Health and Government agencies may place additional obligations on users of their data. UCT requires compliance with these.

7.7.3. Personal data (as defined by Protection of Personal Information Act, 2013 and/or as amended) must be processed, transmitted and stored securely;

- 7.7.3.1. If such data is held on mobile devices (e.g. Smartphones) or removable media, it must be strongly encrypted.
- 7.7.3.2. Other forms of sensitive business data, intellectual property, etc. should, similarly, be strongly encrypted.
- 7.7.3.3. The UCT will issue and keep under review guidance on what constitutes an acceptable standard of encryption.

7.7.4. Any outsourced information services must be subject to a documented contract, which must comply with the guidelines in 3rd Party Supplier Policy.

7.8. Policy Violations

7.8.1. Existing staff and students of UCT, authorised third parties, guests, conference delegates and contractors given access to the UCT network will be advised of the existence of this policy statement and the availability of the associated procedures, codes of practice and guidelines which are published on the UCT website. Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

7.9. Status of the Information Security Policy

7.9.1. This policy statement does not form part of a formal contract of employment with UCT, but it is a condition of employment that employees will abide by the regulations and policies made by UCT. Likewise, these latter are an integral part of the regulations for students.

7.10. Additional policies and guidelines

7.10.1. In order to give effect to information and cyber security at UCT, additional policies, standards, procedures and guidelines for specific information and cyber security focus areas will be published on the UCT web site from time to time.

7.10.2. Appendix A, lists and provides links to current Information and Cyber security related policy and standards

7.10.2.1. Appendix A will be updated and maintained such as to reflect the status of information and cyber security and related policies.

7.10.3. Appendix B provides a listing of policies which are under development or to be developed.

7.10.3.1. Appendix B will be updated to reflect UCT's policy development needs.

7.10.3.2. A policy listed in Appendix B, once adopted is to be removed from this appendix and included in Appendix A.

8. Acknowledgement

8.1. Adapted from

8.1.1. Carnegie Melon University, Information Security Policy, 2008,

8.1.2. Royal Holloway, Information Security Policy 2017 and

8.1.3. The University of Edinburg Information Security Policy 2017

9. Reference

ISO/IEC 27000: 2018 Information technology: Security techniques: Information security management systems -- Overview and vocabulary

ISO.IEC 27001:2013 Information technology: Security techniques: Information security management systems – Requirement

ISO/IEC 27002:2013 Information technology: Security techniques: Code of practice for information security controls

ISO/IEC 27003:2017 Information technology: Security techniques: Information security management systems -- Guidance

ISO/IEC 27004:2016 Information technology: Security techniques: Information security management -- Monitoring, measurement, analysis and evaluation

ISO/IEC 27005:2011 Information technology: Security techniques: Information security risk management

ISO/IEC 27006:2015 Information technology: Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2017 Information technology: Guidelines for information security management systems audit

ISO/IEC 27008:2019 Information technology: Guidelines for the assessment of information security controls

ISO/IEC 27035-1:2016 Information technology: Security techniques-- Information security incident management: Principles of incident management

ISO/IEC 27035-2:2016 Information technology: Security techniques: Information security incident management: Guidelines to plan and prepare for incident response

ISACA, 2012, “COBIT 5 for Information Security”, Rolling Meadows, USA

NIST, n.d., “Glossary of Key Information Security Terms: Version 2”, viewed 4 December 2016, https://csrc.nist.gov/glossary

NIST, 2018, “*Framework for Improving Critical Infrastructure Cyber security Version 1.1*”, viewed 23 March 2019; https://www.nist.gov/cyberframework

10. Appendix A: Current policy and status

The university will from time to time make available supplementary policy, standards, guidelines, procedures and/or codes of practice, and promote them throughout UCT; once approved these will augment this policy and be binding. Appendix A of this policy will be maintained to reflect such additional policy, standards, guidelines, procedures and/or codes of practice.

This policy is amplified by and comprises out of the following policies, sub-policies, standards, guidelines and procedures;

Policy	Document Type	Status	Comments
Acceptable use of Guest Wifi Access	Policy	Approved	
General conditions of service for standard academic staff	Policy	Approved	Last update 25 January 2018 – Clause 16
General conditions of service for Joint Staff	Policy	Approved	Last updated 25 January 2018 – Clause 16
General conditions of service for PASS staff	Policy	Approved	Last update 25 January 2018 - Clause 19
General Rules and Policies 2019 – Student handbook 3	Policy	Approved	Review section on University policies from page 99 onwards with specific refence to ICT
Password Policy	Policy	Approved	9 December 2015
Policy on Securing Electronic Communications using SSL	Policy	Approved	26 May 2017
Policy on Unsecured Computers at UCT	Policy	Approved	25 February 2011
Research Data Management Policy	Policy	Approved	17 March 2018
SAP User Expiry Policy	Policy	Approved	September 2010
Security Incident handling Policy and Procedure	Policy	Approved	28 September 2016
UCT Perimeter Firewall Policy	Policy	Approved	27 March 2012
UCT ICTS Antivirus Policy	Policy	Approved	25 July 2014
UCT Network as a Core ICT Service	Policy	Approved	15 September 2009
UCT Policy and Rules on Internet and Email Use	Policy	Approved	To be replaced by an Acceptable Use Policy. Reference to UCT Policy and Rules in the student handbook to be revised

UCT Records Management Policy	Policy	Published (incomplete)	28 September 2011 Policy is incomplete
Centre for Internet Security Bench Marks	Standard	Adopted	To be made available from and maintained in a central repository
International standards Organisation	Standard	Adopted	To be made available from and maintained in a central repository
Wireless Access for Guests	Guideline	Adopted	n.d.

11. Appendix B: Proposed future policy

Policy	Document Type	Status	Comments
Acceptable Use Policy	Policy	Draft	To replace UCT Policy and Rules on Internet and Email Use
Bring Your Own Device (BYOD) Policy	Policy	To be developed	
Cloud / 3rd Party Code of Practice	Policy	To be developed	
Data Classification Policy	Policy	Draft	
Data Encryption policy	Policy	To be developed	
Data Management Policy	Policy	To be developed	
Data Protection Policy	Policy	To be developed	
Data Retention Policy	Policy	To be developed	
Data Access Control Policy	Policy	To be developed	
Removable Media Policy	Policy	To be developed	
Secure Build Policy	Policy	To be developed	

12. Version tracking

Document Status	Date	Version and change	Author
Draft	17 May 2019	Ver 1.0	Andre le Roux
Draft	18 July 2019	Ver 1.1 Deleted reference to policies yet to be drafted in Appendix A. Proposed deletion of section 7.5.2	Andre le Roux
Draft	6 August 2019	Ver 1.3 changed section 7.3 based on RMC feedback	Andre le Roux
Draft	2 September 2019	Ver 1.2 Introduced section 7.1 through 7.10, renumber section 7.1 to section 7.11, renumbered section 7.2 to 7.1	Andre le Roux
Draft	23 September 2019	Ver 1.4 reworded section 4.1 Revised references	Andre le Roux
Draft	7 October 2019	Ver 1.5 finalised changes as per RMC recommendation. Updated section 7.2.1, revised 7.5.4, Updated contents of Appendix A, added Appendix B and other minor amendments	Andre le Roux
Draft	21 February 2020	Ver 1.6 Corrected typographical and spelling errors	Andre le Roux
Draft	24 February 2020	Ver 1.7 Updated document summary to indicate policy has been reviewed by SEC	Andre le Roux