	UNIVERSITY OF THE WESTERN CAPE		
UNIVERSITY of the WESTERN CAPE	ICT INFORMATION SECURITY POLICY	Council Approval Reference Number	29 June 2017 (C2017/3)
		Implementation Date	TBD
		Revision / Amendment Number	ICS Management
		Revision / Amendment Date	16 May 2017
		Policy Owner	ICS Department
		Executive Management Portfolio	DVC- Academic
		Contributors	ICS Management
		Circulated by:	ICS Management
		Circulated to:	IT Governance Committee IT Portfolio Steering Committee ICS Management

UNIVERSITY OF WESTERN CAPE (UWC)

ICT INFORMATION SECURITY POLICY

DATE OF LAST APPROVAL: C2017/3

TABLE OF CONTENTS

1 DOCUMENT CONTROL

1.1. Preparation

ACTION	NAME	DATE
Prepared by:	Mike Lewis	September 2004
Updated by:	Anver Natha	October 2007
Updated by:	Anver Natha	November 2008
Updated by:	Anver Natha and Conrad Tiflin	March 2013
Updated by:	Anver Natha and Conrad Tiflin	June 2013
Updated by:	Anver Natha and Conrad Tiflin	September 2014
Updated by:	Anver Natha and Conrad Tiflin	December 2015
Updated by:	Anver Natha and Conrad Tiflin	April 2016
Reviewed by:	Tamima Talip	July 2016
Updated by:	Anver Natha and Conrad Tiflin	February 2017
Updated by:	Anver Natha and Conrad Tiflin	April 2017
Updated by:	Anver Natha, Conrad Tiflin, Tamima Talip	May 2017

1.2. Release

VERSION	CHANGE NOTICE	PAGES AFFECTED	REMARKS
1	Initial Policy Formulation and Council Approval	All	
1.1 – 1.7	Updates	All	Terminology, Structure, Content
1.8	Legal Review	All	Content
1.9 – 1.11	Updates	All	Content
1.12	Update based on IT Portfolio Steercom Review	All	Content
1.13	Update based on IT Governance Committee	All	Content

2 Definitions / Acronyms

Common terms and acronyms that may be used throughout this document:

Access Control - Ensures that resources are only granted to those users who are entitled to them.
Authentication - Is the process of confirming the correctness of the claimed identity.
Authorisation - Is the approval, permission, or empowerment for someone or something to do something.
BYOD – **B**ring **Y**our **O**wn **D**evice. Allowance for students, staff, contractors and visitors to utilise their personally owned devices (laptops, tablets, and smart phones) on the UWC network and to access applications and services made available on the network.
Data - shall mean any data, including personal data as defined in the Electronic Communications and Transactions Act, 2002, POPI Act of 2013, and/or any equivalent legislation, or stored, collected, collated, accessed or processed on behalf of the University of the Western Cape.
Encryption – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'
External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, and thumb drives, tapes
Firewall – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.
FTP – File Transfer Protocol.
IT - Information Technology.
LAN – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.
Malware - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.
Segregation of Duties - Is an internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any task.
TLS – Transport Layer Security. A protocol which is used to secure information in transit over computer networks.
User - Any person authorized to access an information resource.

- **Privileged Users –** system administrators and others specifically identified and authorized by Practice management.
- **Users with edit/update capabilities –** individuals who are permitted, based on job assignment, to add, delete, or change records in a database**.**
- **Users with inquiry (read only) capabilities –** individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.

UWC Computer and Network Systems – Include the technical architecture infrastructure (physical or virtual), i.e. networks, operating system platforms, databases, as well as the applications that rely on this to operate.
VLAN – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.
VPN – Virtual Private Network – Provides a secure passage through the public Internet.
WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.

3 Policy Intent

Access to Information is pertinent to the on-going growth and success of the University of the Western Cape ("UWC"). The academic programme, business units and students depend on the systems and applications that provide this information, i.e. "Information Assets", and entrust many individuals with access and the ability to transform data into information and knowledge.

Physical disaster, data leakage, computer malware, systems breakdown, vulnerabilities, fraud and theft could disrupt business operations. Protecting the confidentiality, integrity and availability of information is therefore of utmost importance to UWC and the policy guidelines are put in place to minimise the impact and the likelihood of occurrence for data or information loss.

4 Information Security Policy Compliance

The information security policy and related policies are developed to provide the necessary guidelines to protect information and data at UWC. Failure to comply with the information security policy or other related policies may result in a breach of security. All users of information systems at UWC are required to acknowledge the relevant policies and non-compliance may result in disciplinary action or the withdrawal of the right to use information systems or services at UWC.
The information security policy framework provides UWC with the necessary guidelines that should be followed by all individuals interacting with UWC information systems, including students, staff, as well as external parties and contractors. Every individual or entity has an obligation to appropriately protect information as set out in this document.

In securing information, it is essential that the following characteristics of information are preserved and maintained:

- **Confidentiality** – ensuring that information is accessible only to those authorised to have access.
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods.
- **Availability** – ensuring that authorised users will have access to information and associated assets when required.
- **Legislative and regulatory** – ensuring that adherence to existing and new requirements will be met.

This document aims to align to the ISO 27001 and COBIT 5 standards and strives to comply with the local laws and regulations prescribed within the Republic of South Africa, i.e. **ECT Act of 2002, RICA Act 70 of 2002, and POPI Act of 2013.**

This document supplements and complements existing UWC policies, rules and regulations pertaining to the subject matter and should be read in conjunction with such policies, rules and regulations.

UWC policies are available on the UWC portal and hard copies are obtainable from the UWC Secretariat.

5 Structure and Policy Framework

The policy framework is split into two key focus groups;

- All ICS staff that includes management and the ICT specialists involved in the day-to-day management and execution of IT Processes and functions; and

- All Users including Students, Staff, Contractors, Visitors; the users of information systems and services at UWC.

Furthermore, the framework may comprise three levels of supporting documentation:

- **Individual Policies**: the overarching documents comprising principles and policy statements to be applied within the ambit of management of information;
- **Processes and Procedures**: the implemented processes designed to introduce consistency in the execution of the principles contained within the policies; and
- **Standards**: where appropriate, the acceptable requirements for baseline configuration in the use of technology.

This document makes reference to principles and policy statements only.

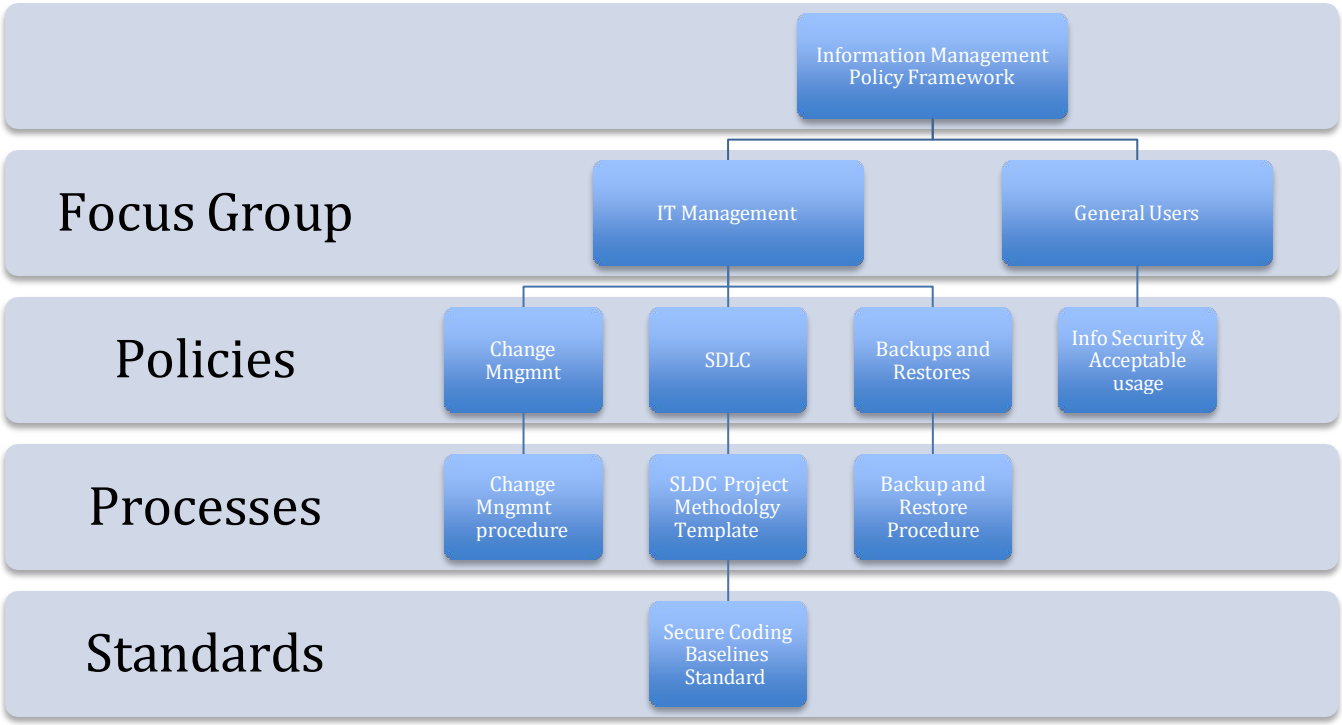

Figure 1: Information Security Policy Framework

6 Scope of this Policy

This policy applies to the following information assets within UWC:

- All information including without limitation electronic and hard copy (physical) information, in all stages of its life-cycle, from creation through entry, processing, communication, dissemination, storage and disposal;

- Electronic information includes:
  - Data processed and stored online, e.g. information on the network, or on a hard drive or portable media;
  - Backed-up data;
  - Archived data, or other off-line storage mechanisms;
  - Audit logs;
  - Data stored on compact discs (CDs) or any portable media, i.e. memory keys; and
  - E-mail.

- Information in print form from UWC Information systems;

7 Roles and Responsibilities

Protecting UWC's information is achieved through multiple responsible parties including:

ROLES	RESPONSIBILITIES
Management	The responsibilities of UWC management include: • accepting accountability for the information assets under their control; • a duty to properly protect its information assets from a variety of threats such as error, fraud, embezzlement, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption, and natural disaster; • providing the appropriate resources, personnel and financial, for information asset protection; • responding to identified exposures and vulnerabilities; • supporting the investigation and resolution of information related losses and incidents; and • ensuring that the Institutions confidentiality agreement/acceptable usage policy is adhered to by all staff, employees and independent contractors.
Information/Business owners	The owner of information is usually the person responsible for the creation of the information or is the primary user of the information. Owners' responsibilities include: • classifying the information; • authorising access to the information; • assigning an information custodian; • specifying and communicating the security requirements; • handling day-to-day security lapses and reporting security breaches to the IT management; • signing and complying with the Institutions confidentiality agreement; and • ensuring that data stored on any local hard drives is satisfactorily backed up and able to be restored as outlined in the institutions data backup and restores procedures document.
Information users	The information user is anyone who is authorised to read, enter (input), update, or delete the information. The user must: • use the information only for the purpose intended by the owner; • report security breaches to IT management (via ICS Service Desk); • not disclose confidential information to anyone without the permission of the owner; and • Digitally Sign (implicitly accepted during login time) and comply with the UWC confidentiality agreement/acceptable usage policy.
Information Custodian	The information custodian is the person responsible for processing or storing the information. The custodian is typically a member of UWC ICS team and is responsible for: • administering the controls specified by the owner; • ensuring proper authorisation is received from the information owner before granting access to information and data; • monitoring network activity for potential security breaches; and • reporting any security breaches to the UWC information security manager.
Contractors/Temporary Staff	All contractors with access to UWC's electronic information should:

ROLES	RESPONSIBILITIES
	• ensure complete awareness of the contents of this policy framework and its implications; • only access those information systems and data specifically authorised; • regard all UWC information collected or accessed during their interaction with UWC as confidential and, as such, may not use, disclose, transfer or amend any information gathered during their stay without the explicit consent of UWC Management; and • ensure that one has familiarised oneself and complies with the UWC non-disclosure (NDA) confidentiality agreement.
IT Security Manager/ Security Team	The role is to: • co-ordinate information protection within UWC under the direction of management (ICS Management Team); • develop and maintain the information security/assurance policy and supporting appendices and standards; • ensure that students, staff, contractors and visitors to UWC are properly educated and aware of this information management policy and its implications on a regular basis; • provide support in planning, implementing and administering information protection measures; • investigate problems; and monitor and report to ICS Management on the effectiveness of information protection measures through the relevant governance committee structures; and • comply with all security measures established.
Internal Audit / Outsourced Partners	It is the responsibility of UWC's Internal Audit department / Independent Co-sourced Audit Companies to audit compliance with this policy's requirements and report to UWC Management on the effectiveness of information protection measures.

8 Policy Statements

8.1 Internet and Email Usage

- Sufficient guidelines should exist to govern the acceptable usage of valuable resources such as UWC computer and network systems, Internet and email services that are made available to staff, students and visitors to UWC.
- These are clearly outlined in the ICT Internet and Email Usage Policy.

8.2 Access Control

- User access to information systems and services require the necessary authorisation from UWC business process owners to gain access to the applicable information system.
- The level of access is role based and given according to what is required to perform one's duties.
- Individual employee logical access to information systems should be reviewed on a regular basis to ensure that permissions granted are still appropriate and to ensure the user access is still valid.

8.2.1 Segregation of Duties

- Information systems that may have a financial impact on the institution requires more than one person to complete a task. The separation and sharing of tasks is a mechanism intended to prevent fraud and error in UWC computer and network information systems.

- No single user should have complete authority and control to perform transactions that may compromise the security and integrity of an information system.

8.2.2 Passwords

- Access to UWC information systems and services will be governed by the use of unique, complex and strong authentication methods.

8.3 Security Awareness and Training

- UWC departments and units should ensure that regular security awareness initiatives are undertaken throughout the University to prevent exposure to information leakage, infection by computer malware, vulnerabilities, fraud and theft of information that lead to disruption of business operations.

8.4 Security Incident Management

- Any breach of an information system that may lead to the information system being compromised whether to fraud, malware, vulnerabilities or exploitation of information should be reported and escalated as a security incident to the ICS Servicedesk.

8.5 Networks

- All network devices, including wireless access points, networked switches, compute infrastructure should be logically and physically secured.
- All wired and wireless networks should be appropriately secured deploying approved encryption and authentication standards.

8.6 Firewalls

- Firewall systems will be deployed to block unauthorised access from external and internal networks to information systems, while permitting outward communication through the Internet.
- All ports (network protocol services) will be closed by default.
- Ports will be opened upon a request, logged to the ICS Servicedesk and accompanied with a formal business motivation.

8.7 Encryption

- All sensitive information that is stored or transmitted should be encrypted using approved encryption algorithms.
- All UWC sites that require login authentication will be secured by TLS certificates.

8.8 Remote Access

- Remote access to UWC information systems will be restricted to the allowed services and functions necessary for users to perform their duties.
- Remote access from off-campus are either restricted to the web services made available or through Virtual Private Network (VPN) services.

8.8.1 Third-Party Access

- Third-Party Access must comply with all information security policy and procedures where applicable.
- Third-party Access to the UWC's information systems must be controlled, documented and approved and are subject to a formal non-disclosure agreement (NDA).

8.9 Anti-Malware

- All UWC compute infrastructure must be supported by anti-malware software installed and scheduled to scan at regular intervals. UWC makes anti-malware software available to all staff and students.

8.10 Physical and Environmental Security

- All information systems should be protected by a physical security perimeter i.e. access control entry gate, manned reception area, secured datacentre, or secured laboratories.
- In the case of workstations and laptops, the ICS department will make cable lock systems available on request.

8.11 Patch Management

- Workstations and servers owned by UWC must have up-to-date operating system level security patches installed to protect the asset from known vulnerabilities.
- This includes all network devices, laptops, desktops, and servers owned and managed by UWC.
- UWC reserves the right to refuse access connection the UWC information systems for BYOD devices that are not appropriately patched.

9 Relaxation and Waiver

- UWC Management may, upon request of an employee, relax any provision of this Policy relating to such employee's use of the UWC Computer and Network Systems.
- Unless otherwise stipulated, such relaxation shall relate only to the specific request received by the employee concerned and shall not be of general application.
- UWC retains the right to take the necessary action as may be required in terms of this policy at any stage.

10 Review

- UWC reserves the right to review and amend this policy document.
- Any such modification shall be automatically effective and shall be deemed to have come to the knowledge of all individuals when posted on the UWC portal.
- The onus is on all individuals to ensure they are fully aware of all policies (and related processes and procedures).
- UWC will endeavour to inform all individuals of changes as and when they occur.
- If any provision of this document is ruled invalid under law, it shall be deemed modified or omitted to the extent necessary, and the remainder of the policy shall continue in full force and effect.

11 Consequences and Violation

- The terms and conditions of this policy have the force and effect of UWC Rules. Contraventions of this policy may expose the user to disciplinary action in accordance with UWC's Rules and Disciplinary Code as amended from time to time.