UWC			
UNIVERSITY of the WESTERN CAPE	**INFORMATION SECURITY AWARENESS AND TRAINING POLICY**	Council Approval Reference Number	C2021/03 (29 June 2021)
		Implementation Date	1 July 2021
		Parent Policy	Information Security Policy
		Version Number	0.3
		Revision / Amendment Date	May 2021
		Policy Owner	Director: ICS
		Executive Management Portfolio	ED – Finance and Services
		Contributors	Refer to revision history
		Circulated by:	ICS
		Circulated to:	**Consultation Channel** / **Date presented**
			IT Portfolio Steering Committee / 01 Feb 2021
			Executive Management Committee / 23 Feb 2021
			UWC Institutional Forum / 30 April 2021
			Senate Executive Committee / 30 April 2021
			Senate Academic Planning / 30 April 2021
			IT Governance Committee / 17 May 2021
			UWC Senate / 25 May 2021
			UWC Council / 29 June 2021
		Approval Date:	29 June 2021

UNIVERSITY OF THE WESTERN CAPE (UWC)

INFORMATION SECURITY AWARENESS AND TRAINING POLICY

DATE OF LAST APPROVAL: C2021/03 (29 JUNE 2021)

This policy should be reviewed and maintained in line with the practices outlined in the 'ICS Policy Framework and Guideline' document.

Contents

1. Introduction

In today's cybersecurity climate, technical controls, although critical, will not be enough to protect the University of the Western Cape's ("UWC") information assets by itself as it will not prevent users from falling victim to cyber scams such as phishing, amongst others. People are the weakest link when it comes to security therefore an effective Awareness and Training (hereafter "A&T") program can reduce the risk of cyber attacks which vary from phishing to ransomware attacks.

1.1 Purpose

This Policy serves as a functional policy that underpins the overarching Information Security policy. The purpose of this policy is to educate users on their responsibility to help protect the confidentiality, integrity, and availability of UWC's information assets.

This Policy must be read in conjunction with other applicable policies as listed in section 6 of this document.

1.2 Applicability and Scope

This policy applies to all UWC functional lines that have a responsibility towards the development, execution and maintenance of information security (hereafter "InfoSec") awareness and training programs.

The scope of this Policy includes all users that have access to UWC's information assets.

2. Definitions

"Must"	"Must" imposes a legal obligation on the reader implying that something is mandatory.
"Will"	"Will" is similar to "must" however implies a future obligation.
"Should"	"Should" implies that the reader has a choice, i.e. there may be a valid reason to bypass a requirement, however the full implications must be understood and carefully assessed before choosing a different recourse.
"Establish"	For the purposes of this policy, "establish" implies defined (documented) and implemented.
Content delivery channels	May take the form of classroom-based A&T, online training platform (e.g. eLearning), banners on TV screens, videos, posters, emails, events, etc.
InfoSec A&T plan	A plan outlining at a minimum the InfoSec A&T topics, mandatory vs recommended sessions, the target audience, the facilitators or trainers whether inhouse or outsourced, the content delivery

	channels, the A&T material to be customised per stakeholder group based on relevancy to their roles, planned dates, venues and assessment methods.
InfoSec A&T material	May include basic information security content such as: • Common InfoSec and cyber-specific threats • How to recognize and avoid these threats • What to do in the event of a successful breach and where to report potential and actual instances • Data handling requirements for users that have access to classified information.
IT	The Information Technology (IT) department that is responsible for delivering Information and Communication Technology (ICT) services to the UWC community.
High risk user groups	May include user groups such as privileged users, i.e. those with elevated access such as network/system/application/database administrators, developers, super users or users with access to classified information as per the Data Classification Standard, Senior executives and their personal assistants (PA's) as they are typically targets for whaling attacks and third parties who have access to and/or process UWC classified information.
Information asset	Any information or data that is of value to UWC whether in electronic or hard copy format and if its security is compromised, it would have a significant impact on the institution's business operations.
Systems	UWC's information systems including network, operating system, application or database software.
Classified information	UWC's Sensitive, Confidential and Internal data that requires a higher level of protection as defined in the Data Classification Standard.
Phishing	A type of social engineering attack often used to steal user data such as login credentials and credit card numbers. An attacker pretends to be a trusted entity to dupe a victim into clicking a malicious link, that can lead to the installation of malware, freezing of the system as part of a ransomware attack, or revealing of sensitive information.

Ransomware attack	Malicious software that infects your computer and locks your computer screen with a display message demanding a fee to be paid in order for you to gain control over your system again.
Users	Any person (e.g. UWC student, staff, third party, etc.) who has been authorised to access UWC's information assets and related systems.
UWC functional lines	For the purposes of this policy, functional lines refer to all functional line management (Academic, Admin and Support areas) that have staff reporting to them as well as academic staff that manage students.
Whaling attack	A type of phishing attack that targets high profile individuals.

3. Policy Statements

3.1 Requirements gathering: A&T requirements for InfoSec must be identified as inputs into the program. This should include at a minimum, any topical or high risk issues that are prevalent in the UWC environment and the Higher Education sector, and an understanding of the university culture and the target audience that require A&T.

3.2 A&T Program development: An InfoSec A&T program, plan and supporting material must be developed and critical success factors and metrics must be established for measurement and reporting.

3.3 Executive Management support: Executive management buy in and support of the A&T program must be obtained prior to executing the program.

3.4 Execution of A&T program: The program should be executed through planned A&T campaigns:

3.4.1 Practical exercises in InfoSec and privacy should be included where possible to reinforce training objectives.

3.4.2 The A&T material must reinforce the principles from the suite of InfoSec policies and standards.

3.4.3 Collaboration with external stakeholders or special interest groups should be encouraged for staff with InfoSec responsibilities to achieve broader InfoSec awareness from an industry, national and global perspective.

3.4.4 All UWC staff, students and third parties must be given general A&T, however high risk user groups must be identified for role-based training in terms of their job responsibilities.

3.5 Monitoring effectiveness of A&T program: The A&T program must be tested for effectiveness on a periodic basis.

4. Policy Compliance

Refer to the overarching Information Security Policy for compliance measurement, non-compliance and exceptions to the policy.

5. Roles & Responsibilities

All users are responsible for Information Security and their responsibilities are outlined in the Acceptable Use policies for UWC staff and students and in contractual agreements for third parties. All functional lines across Academic, Admin and Support areas will be responsible for the development, execution and maintenance of their respective InfoSec A&T programs and where necessary, the IT and HR departments' resources and processes (e.g. HR onboarding / induction process) can be leveraged to deliver on these programs.

Key responsibilities in respect of this policy	*IT GRC	*IT Dept	*HR Dept	Functional lines	Audit	*EMC	*ICT Portfolio SteerCom	*ICT GC	Council
Maintain (review and update) this policy.	R	C	C						
Approval of this policy.						R	R	R	R
Communicate and create awareness of this policy and any subsequent changes.	R		R			C	C	C	C
Establish standards, processes, procedures and controls to support this policy.	R	R	R	R					
Ensure implementation of policy and remediate risks within area of responsibility.	C	C	C	R(1)		C	C	C	C
Risk assessments – assess risks associated with this policy and track the management and remediation of risks.	R	C	C	C		C	C	C	C
Policy compliance measurement – assess compliance to this policy.	R	C	C	C		C	C	C	C
Audit key controls and report on the design and effectiveness of the control environment.	C	C	C	C	R				

*GRC = Governance, Risk and Compliance *IT = Information Technology, *Dept = department, HR = Human Resources, EMC = Executive Management Committee, SteerCom = Steering Committee, ICT GC = Governance Committee, R = Responsible, C = Consulted

Notes:
(1) The IT and HR departments also form part of functional lines and will therefore still be responsible for ensuring the implementation of this policy for their respective areas.

6. Related internal documents, industry standards and legislation

- **Internal documents:** Information Security Policy (C2021/03), Acceptable Use Policy (C2021/03), Data Classification Standard
- **Industry standards:** ISO/IEC 27001:2013
- **Legislation:** Protection of Personal Information Act 4 of 2013, Electronic Communications and Transactions Act 25 of 2002.

7. Revision History

Version	Date of change	Summary of Change	Changed by
0.1	November 2020	Created the policy in alignment with industry standards and legislative requirements as listed in Related internal documents, industry standards and legislation as well as the 'ICS policy framework and guideline' to ensure standardisation across all ICT policies.	Ilhaam Gihwala
0.2	May 2021	Updated the policy cover page to reflect stakeholder consultation	Gail Francke
0.3	May 2021	• Updated the 'circulated to' section in the cover page table to be in date order sequence • Updated Senate date from 23 Feb to 25 May 2021	Gail Francke