	University of the Western Cape		
UNIVERSITY of the WESTERN CAPE	**PASSWORD POLICY**	Document Type	Policy
		First Council Approval Reference Number	C2005/03 – 26 January 2005
		Implementation Date	27 January 2005
		Latest Revision / Amendment Number	**C2023/02 – 22 June 2023**
		Implementation Date of Amended Policy	**23 June 2023**
		Provisos (if any)	None
		Policy Owner	ED: Finance and Services (ICS)
		Portfolio	ED: Finance and Services
		Contributors	ICS, IT Portfolio Steering Committee, EMC, IT Governance Committee, Senate, Council.
		Circulated by:	ICS Governance, Risk and Compliance
		Circulated to:	Campus Community

UNIVERSITY OF THE WESTERN CAPE (UWC)

PASSWORD POLICY

DATE OF LAST APPROVAL: C2023/02 – 22 JUNE 2023

TABLE OF CONTENTS

1 Introduction

Passwords are an important aspect of computer security and are broadly used to access IT resources, and provides the frontline of defense against unauthorised access. Good password management can minimise the likelihood of unauthorised access and user accounts being easily compromised leading to a breach of the University's information and IT systems. A poorly chosen password may result in the compromise of the network of the University of the Western Cape (UWC). As such, all UWC employees, including contractors, vendors and visitors with access to UWC IT systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The University has an obligation to comply with relevant South African statutory, legal and contractual requirements. The Password Policy is part of the Information Security suite of policies, designed to ensure that user passwords and access are managed properly to mitigate risks to the confidentiality, integrity and availability of University information and information systems.

The Password Policy incorporates principle-based guidance provided by The National Institute of Standards and Technology (NIST), which is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce and provides research and guidance on a number of Technology matters, including Information Technology and Cyber-Security.

1.1 Purpose

This Policy serves as a functional policy that underpins the overarching Information Security ("InfoSec") policy. This policy and supplementary policy documents aim to promote and enforce compliance with applicable laws by providing directions on good information security practices to underpin the University's compliance with these laws as listed in Section 6 of this document.

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

1.2 Scope

This policy applies to all UWC staff, Council members, students, third parties and guests who have access to UWC's ICT resources. The scope of this Policy includes all UWC-owned IT equipment, systems and information assets (collectively referred to as "ICT resources").

Exclusions and constraints:

- Institutional dependencies may impact the IT department's ability to implement some of the security safeguards, but IT will endeavor to optimise its resources to achieve the principles outlined in this Policy.
- Owners of BYOD must manage the configuration on their own devices in line with the minimum security configuration guidelines provided by the IT department.

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.
Devices	Any wired or wireless (mobile) computer device connecting to UWC's network such as desktop computers, laptops, mobile phones, tablets, printers, etc.
"Establish"	For the purposes of this policy, "establish" implies defined (documented) and implemented.
IT	The Information Technology (IT) department that is responsible for delivering Information and Communication Technology (ICT) services to the UWC community.
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**.
Third party supplier	An external party (organisation) that supplies goods or services to UWC.
Users	Any person (e.g. UWC student, staff, third party, etc.) who has been authorised to access UWC's information assets and related systems.
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.
Authorised Users	All users who access, handle, process, store, share or manage the University's information assets based on a valid business need. This may include University staff, students, contractors and third-party agents.

Default password	A default password (usually "123," "admin," "root," "password," "<blank>," "secret," or "access") is a standard preconfigured password for a device or software. Such passwords are the default configuration for many devices and, if unchanged, present a serious security risk. Default passwords are intended to be placeholders and used only for the initial setup of hardware or after a factory reset.
Privileged (Super) Users	System administrators and others specifically identified and authorized to have elevated administrator system rights.
BYOD	Bring Your Own Device is a practice of allowing employees of an organisation to use their own computers, smart phones or other devices for work purposes.

3 Policy Statements

3.1 General Statements

3.1.1 Password rules for the creation of passwords are defined in the Password Standards for User Accounts and Password Standards for Super User Accounts, and these should be read in conjunction with this document.

3.1.2 The UWC Minimum Password Standard for User Accounts provide the minimum level of acceptable requirements that must be achieved through execution of processes ensuring standardisation across the institution.

User Accounts:
The accounts that are used for day to day access to systems and applications:

Minimum password length	10 characters	The minimum password length configured by policy.
Password complexity	Upper and lower case alphabetic Numeric Special characters	Choose 3 of the 4 complexity requirements
Maximum number of invalid login attempts	3	Account is locked out after 3 login failures
Password expiry days (age)	180 days	The password must be changed by the user after 180 days.
Minimum number of days between password changes (age)	1 days	The user is allowed to change their password one (1) day after a previous password change.
Password History	12 passwords remembered	Password history prevents reusing recently used passwords.

3.1.3 Default passwords must be changed prior to deploying any IT system.

3.1.4 All passwords must be changed as per the frequency defined in the above-mentioned Standards documents.

3.1.5 All system administrator passwords must be stored in a password vault or equivalent where access is restricted.

3.1.6 All passwords must be changed immediately where there is reason to believe that the password or account has been compromised.

3.1.7 All passwords must be treated as confidential information and must not be shared with anyone or made public in any form, verbal or written.

3.1.8 The same passwords must not be re-used for multiple University IT systems.

3.1.9 Where a group of users requires access to a system, each user must be provided with unique login details to that system.

3.1.10 Privileged account users such as IT systems administrators and support staff must have separate accounts and passwords which are different from their day to day user accounts.

3.1.11 For an approved third-party system that requires the use of the University email address or user ID as part of its authentication, the University user password must not be used on such systems unless single sign on or federation is available.

3.1.12 Where system monitoring makes use of SNMP or similar protocols, the community strings or access keys must not be default, such as “public,” “private” and “system” and must comply with UWC Password Standard and Guidelines.

3.1.13 Any user suspecting that his/her password may have been compromised must report the incident to the UWC Service Desk (servicedesk@uwc.ac.za) and change all passwords.

3.1.14 University login details must not be used for personal interaction with social media or other (non-university) related sites such as Facebook.

3.2 Application development

Application developers must ensure that their programs contain the following security precautions:

3.2.1 University applications must not store passwords in clear text or in a reversible format.

3.2.2 Applications must not transmit passwords in clear text.

4 Policy Compliance

4.1 Compliance Measurement

ICS will take proactive measures to assess compliance to this policy internally through periodic control assessments.

4.2 Non-Compliance

Contraventions of this policy may be subject to the UWC Code of Conduct and HR Disciplinary Processes. Violations of this policy include, but are not limited to:

- Enabling unauthorised individuals to access information;
- Disclosing passwords in a way that violates applicable policy;
- Inadequately protecting passwords;

Failure to adhere to the Password Policy may result in network and application access revocation, further corrective action, and/or civil or criminal prosecution. Violations may be subject to disciplinary action pursuant to University policies and procedures.

Non-compliance by Third Parties may result in the loss of access or the suspension of access until a review can be performed.

Exceptions

Where it is not possible or practical to apply or enforce any part of this policy, a formal request must be submitted with justification to the IT Service Desk (servicedesk@uwc.ac.za). Policy exceptions will be granted in the form of a risk acceptance, and signed by the Head of ICS. Risk acceptances must only be granted for specified periods of time and must be reviewed annually.

Policy Review and Maintenance

This policy will be reviewed and updated periodically (at least every two years, or sooner, considering changes to statutory laws, business requirements or contractual obligations) to ensure that it remains appropriate.

5 Roles & Responsibilities

From a governance perspective, the overall accountability for institutional-wide Information Security lies with the UWC Council and the Rector is in turn accountable to the Council.

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

*IT GRC = IT Governance, Risk and Compliance, EMC = Executive Management Committee, SteerCom = Steering Committee, IT GC = IT Governance Committee, R = Responsible, C = Consulted, A = Accountable, I = Informed

6 Related internal documents, industry standards and legislation

- **Internal documents:** UWC Password Standard for User Accounts (ref no.), UWC Password Standard for Super User Accounts (ref no.), Data Classification Standard (ref no.).
- **Industry standards:** ISO/IEC 27001/2:2013
- **Legislation:** Protection of Personal Information Act 4 of 2013, Promotion of Access to Information Act 2 of 2000, Electronic Communications and Transactions Act 25 of 2002, UWC Institutional Statute, 7 September 2018, Part 1 of 4 in accordance with section 33 (1) of the Higher Education Act, 1997 (Act No. 101 of 1997 as amended).

7 Revision History

Version	Date	Summary of Change	Date of Next Review
Amendment 1	11/2021	• Aligned the policy with industry standards and legislative requirements as listed in Related internal documents, industry standards, and legislation. • Updated the structure of the policy and policy statements in line with ISO27002 control domains and requirements. • Aligned the policy with the 'ICT policy framework and guideline to ensure standardisation across all ICT policies.	November 2026
Amendment 2	01/2022	• General review and amendments in line with update guidance from NIST	January 2027
Amendment 3	22/06/2023	• Included the user password standard requirements in line with governance committee stakeholder recommendations	June 2028