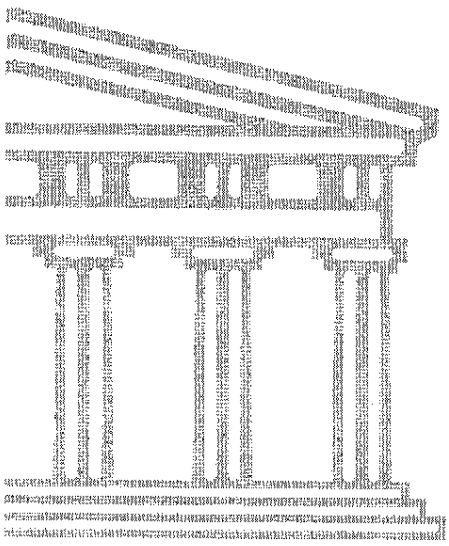
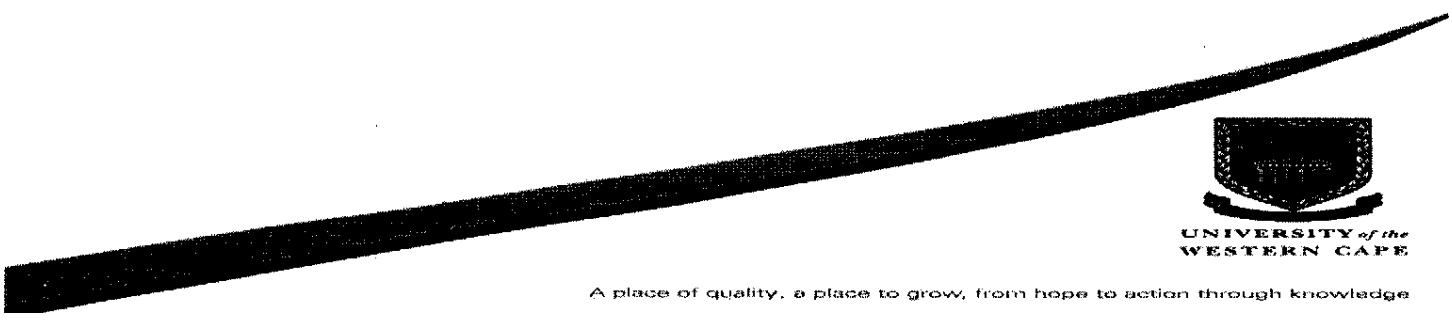


UNIVERSITY OF WESTERN CAPE (UWC)

IT SECURITY POLICY

DATE OF LAST APPROVAL: C2004/5



University of the Western Cape
IT Security Policy

University of the Western Cape Policy *ICS/2004.04*

1. INTRODUCTION

a. General Information

Access to sensitive university information by unauthorised persons could result in legal liability, substantial financial loss, violation of personal privacy and embarrassment to the university. The campus networks, which connect to the outside world through the Internet, are no longer isolated from the potential of unauthorised access. With an increasing use of computers and networks on campus and with people worldwide having access to the university network, it is important that the University of the Western Cape (UWC) implements controls to protect access to university information and data.

b. Objectives

- The University of the Western Cape recognises that information is an asset and vital to the academic and economic well being of the institution, and will therefore create security measures and assign responsibilities to protect this asset from loss, theft, and unauthorised modification or disclosure.
- All security measures must conform to established university policies and legal requirements.
- Every cost effective measure will be made to ensure confidentiality, integrity, authenticity and availability of information.
- It is a priority for all employees at all levels of the University to protect the confidentiality, integrity, and availability of information resources.

c. Purpose

The purpose of the security policy is to:

- Establish direction, procedures and requirements to ensure the appropriate protection of information handled by the university computer resources.
- Emphasise the importance of security in the various computer environments and the role of staff and students in ensuring that security.
- Assign specific responsibilities for the provision of data and information security.

d. Scope

This policy applies to all university owned information or data in all forms including electronic or physical.

The policy applies to all permanent, contract and temporary employees, students, contractors, consultants and other workers at the .university, including those affiliated with third parties who access the university computer network.
The security policy applies equally to networked servers, stand alone computers, peripheral equipment, personal computers, laptops or workstations within UWC and equipment outside of the university network but authorised for access to the university resources.

Resources include data, information, software, hardware, facilities and telecommunications.

2. RESPONSIBLE ORGANISATIONAL STRUCTURE

The Office of the Executive Director for Information and Communication Services (ICS) will be responsible for this policy and for any appeals of ICS decisions relating to the security policy. This policy will be reviewed yearly by ICS, and authorised changes will be effected through approval of the Information Systems Committee (CISC).

3. SECURITY STANDARDS

a. Confidentiality

Confidentiality refers to the university's needs, obligations and desires to protect private, proprietary and other sensitive information from those who do not have the right and need to obtain it.

b. Integrity

Integrity refers to the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.

c. Authorisation

Authorisation refers to whether a particular user, once identified is permitted access to a particular resource.

d. Access

Access defines rights, privileges, permissions and mechanisms to protect assets from access or loss.

e. Appropriate use

IT Systems may be used only for their authorised purposes -- that is, to support the research, education, administrative, and other functions of the University of the Western Cape. The particular purposes of any IT System as well as the nature and scope of authorised, incidental personal use may vary according to the duties and responsibilities of the User. Users are entitled to access only those elements ofIT Systems that are consistent with their authorisation.

4. PERIMETER SECURITY

a. General

The statements under general will apply to all areas within the perimeter security policy.

1. Users will be granted access to the UWC private network by means of network authorisation.
11. ICS may deploy mechanisms that will track user activity as regards to unauthorised access to IT systems

b. Internet Service Provider (ISP) Router

TENET, the university ISP, controls access and security to the ISP router. TENET security policy restricts the university from gaining any access to the router.

c. Firewall

ICS will deploy firewall/s to protect the university internal network and IT systems from unauthorised access.
The firewall policy includes the following

1. The University adopts a closed port policy with the requisite authorisation being required to open ports for services.
ii. The Firewall/s should be transparent to internal users so that users may perform all allowed network services without undue disruption.
111. The Firewall/s should permit or deny services to specific Internet Protocol (IP) addresses.
1v. The Firewall/s should have auditing capability so that user access can be tracked or audited when necessary.

d. Demilitarised Zone (DMZ)

The DMZ network is a semi trusted area for all public facing servers. The UWC web servers and any other public access servers will be assessed against baseline configuration standards to ensure system security before being placed in the DMZ.
The DMZ network can be extended beyond the ICS data centre to selected locations provided valid business or academic needs exist.

Servers installed within the extended DMZ needs to be secured by the department hosting the servers.

e, Intrusion Detection Systems

UWC will deploy Intrusion Detection Systems to identify and prevent intrusive or malicious network activity. In addition, operating system, user accounting, and application software audit logging processes will be enabled on all host and server systems. Audit logs from the various systems will be regularly monitored and corrective action taken.

f. Public Access Servers

All public facing servers will be secured and hardened as per the best practices of the operating systems vendors.

Microsoft Servers
Hardening of Microsoft Web Servers as per Microsoft recommendations currently available at http://go.microsoft.com/fwlink/?Linkid=l4846 or such additional recommendations as made from time to time.

Free UNIX Servers
All services that are not required will be disabled.
Only secure authentication will be permitted.
Patch Management to secure servers to be carried out as per recommendations for the respective operating systems

g. Remote Access

Modems for dial up access will not be allowed on computers or servers which connect to the University network without the consent of ICS. Stand alone computers with modem connections must be registered with ICS. Systems which have access to both modem dial up and the university network pose a security risk

5. INTERNAL SECURITY

a. Physical Security

Physical security refers to the protection of equipment and all information and software contained therein from theft, vandalism and accidental damage. The datacentre where most mission critical servers and communication equipment is held, is a controlled environment with reliable power supplies, adequate climate control, and appropriate secure access.

1. Equipment located in publicly accessible areas that cannot be locked should be fastened down with a cable lock system or enclosed in a lockable computer case.

b. Access Control

i. Department Heads must ensure that revised access rights to IT systems are communicated to ICS when user access requirements change.

11. All access requests and changes will be subject to ICS change control procedures

111. Physical access to the datacentre and designated equipment are restricted to authorised personnel only.

1v. Network authorisation will be required by remote users for access to the university internal network.

c. User Accounts

1. Each authorised user on the university network will be issued with a unique login account commonly known as the network identity

11. Users are only permitted access to university computers using their unique network identity and no shared logins are permitted.

111. Dormant network accounts will initially be locked before permanent removal..

d. Passwords

1. Procedures regarding usage of password and network accounts for the various systems will be published by ICS

ii. Users are required to use passwords to gain access to IT systems including their desktop computers.

e. Data Backups

1. Data will be backed up regularly and stored securely for purposes of data recovery purposes. ICS has backup policies that outlines the backup and restore procedures as is currently used.

f. Disaster Recovery Plan (DRP)

1. The university will produce a DRP plan which will outline the recovery of IT systems in an emergency. A DRP simulation test will be conducted at least once a year to test ICS readiness.

g. Change Control

1. All computer and communications systems used in production employs a formal change control process whereby changes to the production environment are initiated. The Change control process is used for all significant changes to software, hardware, communication links and procedures.

h. Virus Protection

Additional information on Virus protection is available in the UWC Virus policy.

1. All of the university servers and desktop computers must have up to date virus protection software installed.
11. Virus checking must be done on all files downloaded from external sources, disks or CD's.
111. Anti-virus software must be updated shortly after a new version is made available.
1v. Certain file types may be prevented access to the university via email as a necessary precaution against email borne viruses.
v. ICS will deploy anti-spam procedures to minimise or prevent spam mail from entering the university.

i. E-Mail

i. The Universities E-mail system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
11. ICS may introduce mechanisms to prevent unsolicited mail or content deemed as undesirable by the university executive.

Approved by Council on 4 December 2004 (C2004/5)