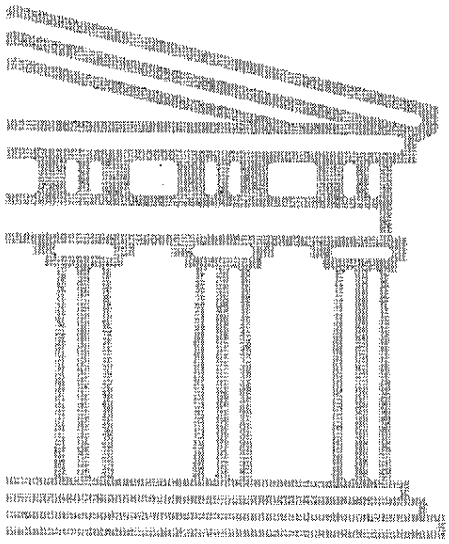

UNIVERSITY OF WESTERN CAPE (UWC)

PHYSICAL ACCESS POLICY

DATE OF LAST APPROVAL: C 2005/3

 Policies & Procedures	**Date:** 3 March 2005	Draft 1
	Revision Date	**Revision No**

SUBJECT: INFORMATION & COMMUNICATION SERVICES

POLICY TITLE: PHYSICAL ACCESS POLICY

Physical Security Policy

Overview

Technical support staff, security administrators, system administrators, and others may have ICS datacentre facility physical access requirements as part of their function. The granting, controlling, and monitoring of this physical access to ICS facilities is important to an overall security program.

Purpose

The purpose of the ICS Physical Access Policy is to establish rules for granting, monitoring, and removing physical access to the ICS datacentre and network infrastructure components.

Scope

The scope of this policy applies to anyone with physical access to the datacentre and network infrastructure components of the Information and Communication Services department (ICS). This includes technical support staff, security administrators, system administrators, others that are responsible for the installation and support of Information and Communication Technology (ICT) services, and data owners

Policy

- All physical security systems must comply with all applicable regulations such as, but not limited to, building regulations and fire prevention regulations.
- Physical access privilege to all ICS facilities must be documented and managed.
- All ICS facilities must be physically protected in proportion to the criticality or importance of their function.

- Access to the datacentre facilities must be granted only to UWC or ICS support personnel and contractors whose job responsibilities require access to that facility.
- The process for granting card and/or key access to ICS datacentre facilities must include the approval of the person responsible for the facility.
- Secured access devices, such as access cards, keys must not be shared or loaned to others.
- Secured access devices that are no longer needed must be returned to the person responsible for the facility and the return logged. Secured access devices must not be re-allocated to another individual bypassing the return process.
- Lost or stolen secured access devices must be reported to the person responsible for the ICS datacentre facility immediately.
- The person responsible for the ICS datacentre facility must remove the secured access rights of individuals that change roles within ICS or are separated from their relationship with it.

Practices

- Visitors should be escorted and/or monitored in secured access controlled areas of the ICS datacentre.
- The person responsible for the datacentre facility should review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the datacentre facility must review secured access device rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Security controls must not be bypassed or disabled.
- Security awareness, emergency evacuation of personnel must be continually emphasized, re-enforced updated and validated

Disciplinary Actions

- Violation of this policy may result in disciplinary action for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or suspension or expulsion in the case of students. Additionally, individuals are subject to loss of ICS access privileges, civil or criminal prosecution.

Council APPROVED the report including the following strategy and policies:
Bandwidth Management and Acquisition Strategy;
Physical Access Policy;
Password Policy; and
Internet and Email Usage Policy Applicable to Laboratories and Resource Centres.
- DECISION TAKEN