UNIVERSITY OF PRETORIA
Department of Security Service

ACCESS CONTROL POLICY

Document type: Policy   Document number: Rt 205/22
Policy category: Security Services

CONTENTS

1. **Purpose** 1
2. **Scope**....2
3. **Consequence of non-compliance** 2
4. **Policy statement** 2
5. **Definitions**....3
6. **Principles**....3
6.1 **Access to University of Pretoria premises**....3
6.2. **Additional access rights**....4
6.3. **Access for Contractors/academic Visitors and long term Sponsored guests**....5
6.4. **Centralised access control system (ACS)**....6
6.5 **Visitor Management System (VMS)**....6
7. **Roles and Responsibilities**....7
8. **Associated documents**....8
9. **Policy life cycle** 8
10. **Document metadata** 8

1. Purpose

The purpose of the policy is to provide general rules and guidelines relating to physical access to all UP controlled premises, which includes but are not limited to campuses, residences and sport grounds.
Different access rules apply to the diverse categories of persons requiring access to UP, e.g.:

- Students
- Staff
- Visiting researchers

- Service providers, contractors and sponsored guests
- Different types of announced and unannounced visitors: parents, prospective students etc.
- Active card holders not in possession of the card at the time requiring access.

The University of Pretoria has a centralised access control system (“ACS”) supporting the regulation of access to all campuses, residence areas, buildings, labs etc. All perimeter access to campuses and residences requires dual verification (proximity card and biometric readers) and the access card used is a smart card. To provide a process which allows users without access cards to enter UP premises, by making use of scanner devices to record visitor information from an independent form of barcode ID or e-passport. The Visitor Management System (“VMS”) was implemented for this purpose.

The purpose of the access control policy and related visitor management guidelines are to manage access to and egress from campuses, residences and buildings to improve safety and security on all controlled premises of the University of Pretoria.

This policy sets out the roles, responsibilities, principles and guidelines that the University established, maintains and developed, in order to ensure the safety and security of individuals and property.

2. Scope

This is a University-wide policy which applies to all staff members, students, visitors, contractors and guests on all controlled premises of the University of Pretoria.

3. Consequence of non-compliance

Non-compliance can result in a breach in security measures. Students, staff, contractors, guests and visitors not adhering to the policy may be denied access to UP controlled premises.

4. Policy statement

The University will endeavour to ensure, as far as is reasonably practicable, the personal safety and security of all students, staff, contractors and visitors at all University-controlled premises.

The Department of Security Services is tasked with and fully committed to maintaining a safe and secure environment that allows students and staff to study, teach, learn, conduct research, work and participate in sport, cultural and social activities.

Through the implementation of this policy, the University, within its ability, commits itself to create a safe environment that ensures safety of persons and property, thereby enhancing the University experience for students, staff, contractors and visitors.

5. Definitions

Biometrics	A way of measuring and using an individual's physical characteristics for verifying his/her identity
Campus	Any of the campuses of the University
Contractor	Any person or company contracted by the University or as a sub-contractor by any service provider to the University
Minor children	Persons under the age of 18 years
Multi-time PIN (MTP)	A scanner-friendly alphanumeric code that allows multiple entries
Smart card	A plastic card with an embedded computer chip
Sponsored guest	A person requiring access to a UP premises sponsored by a UP personnel member post level 6 and higher
Staff	Any person who is permanently or temporarily employed by the University
Student	Any student registered at the University
One-time PIN (OTP)	A scanner-friendly alphanumeric code that allows a single entry
Policy	A set of principles to guide actions.
the University	University of Pretoria
Unwanted individual	A person who has been suspended or dismissed, or whose employment or studies with UP has been terminated
Visitor	A person who is not a student, contractor or a staff member of the University who require access to a UP controlled premises

6. Principles

6.1 Access to University of Pretoria premises

The access control policy is guided by the following principles:

- Students, Staff, Contractors and other UP access card users are allowed access to UP premises by using the Biometric and Smart card access control system at the turnstiles/boom gates to the premises.
- Invited/announced Visitors will receive a One-time PIN code or a barcode for a particular day, which will be scanned together with a valid South African ID, passport or driver's licence to gain access to the premises. For Visitors driving vehicles, the number of passengers will be captured and the vehicle's licence disk barcode scanned.

- Invited / announced Visitor groups can apply to Security Services, Security Systems and Technology Unit to be issued with a One-time PIN or multi-time PIN's.
- Any non-Smart cardholder/unannounced Visitor must prove their identity by presenting a valid identity document, driver's licence or passport at the official visitor desk upon entering and exiting the University's premises. The officer will process the Visitor by scanning the South African ID or driver's licence or passport using a portable security scanning device. For Visitors driving vehicles, the number of passengers will be captured and the vehicle licence disk barcode scanned. The visitor register will also be completed by the Visitor.
- Identity documents of all passengers in a vehicle will be scanned on entering and exiting the campus, excluding Minor children.
- Once a person enters the University of Pretoria's premisses, the general rules and regulations and policies of the University is applicable to him/her.
- Any person who refuses to make use of the Biometric and Smart card access control system will be denied access to the University's premises.
- Any person who refuses to provide valid identification will be denied access to the University's premises.
- Staff members may only issue PINs after they have received permission to do so from their HODs or Directors and Security Services.
- Staff members are responsible for ensuring that their guests are aware of and accept the applicable rules, regulations and policies of the University.
- Visitors to whom PINs have been issued may be refused entry if their names appear on Security Services' list of Unwanted individuals.
- Any Staff member, Student, Contractor or Visitor who has been accused of or charged with any form of gender-based violence or sexual harassment may be refused access to any University controlled premises.
- Individual cases of persons without Biometric readings such as (fingerprints, iris, proximity finger print scanners etc) will be managed by the Department of Security Services.
- Depending on the situation, the business rules for the ACS and VMS and deployment thereof can be adopted to manage emergency situations.
- The University reserves the right to change the conditions of access rights, implement new systems or put additional measures in place to ensure a safe and secure study and work environment.

6.2. Additional access rights

- Motor vehicle access is obtained through the successful application, receipt and acknowledgement of receipt of a parking disc. Different rules apply for Staff, Students and Contractors, as well as the various UP premises. The Traffic and Parking Management rules and regulations will also be applicable and should be complied with.
- No diplomatic vehicles will be allowed to use any University premises as thoroughfare. The parking disc rules and regulations apply to all Students, including Students who are diplomats.
- Any Student, Staff member or Contractor authorised to drive UP vehicles can obtain vehicle access, regardless of whether this person has a parking disc for a certain period of time. The Department of Facilities Management will assign an affiliation, which will

activate the access card at all motor gates at Campuses (excluding residences), for the approved period only.

- Staff and Students have default access rights to the libraries and open laboratories of the University.
- Staff, masters and doctoral Students have default access rights to the research facilities in the libraries.
- Additional access to buildings, venues or laboratories must be requested in writing by the HOD or an authorised Staff member of a department or faculty to the Department of Security Services.
- Access to residences is managed by the Department of Residence Affairs and Accommodation. Only Smart cards of Students officially placed in residences are activated for the respective residence pedestrian gates. Motor vehicle access to residence premises is obtained via residence parking discs.
- All access cards are de-activated during the December recess period, unless otherwise communicated.

6.3. Access for Contractors/academic Visitors and long term Sponsored guests

- Any person who is not a registered Student or an appointed Staff member will receive a Contractor category card. The Contractor / Sponsored guest category cards are issued to professional persons associated with the University, (but who are not employees of the University), such as guests, consultants, dependants of residence personnel, persons employed by residence personnel in their personal capacity, other persons associated with the University, as well as service providers. Each of these card applications must be authorised by a UP Staff member, post level 6 and higher, responsible for these card holders.
- Applications for card access for this category of person must be done on Permission Manager on the UP portal.
- Any visitor who plans to gain entry on more than five days within a two-month period must apply for an access card on Permission Manager.
- Provision is made for different categories of guests, some of which are:
  - Academic visitors
  - Alumni donors
  - Persons remunerated on claims basis
  - Consultants
  - Contractors listed under a service provider company
  - Council members
  - Pensioners
  - Members of TuksSport sportclubs or other social or cultural clubs
  - Visitors to the high performance centre and Future Africa
  - Visitors to TuksSport high school
  - Different categories of postgraduate Students who require access prior to registration.

6.4. Centralised access control system (ACS)

- Depending on the situation, the rules for the ACS and VMS and the deployment thereof can be adopted to manage emergency situations.
- The ACS makes provision for persons with special needs and disabilities. Applications are managed by the Department of Security Services.
- Misuse of the ACS or VMS or contravention of rules applicable to access to UP premises may lead to disciplinary action.
- Any Biometric or Staff information captured in the ACS will be used for access control purposes only.
- The ACS and VMS are not a time and attendance programme and will not be used for this purpose.
- Any log files and transactions for a particular person may be requested by the Department of Human Resources (Employee Relations) or the UP-Information Officer, the Office of the Registrar or the Internal Audit division for a formal investigation, or, in the case of a Student, the Registrar's Office. No data will be supplied to any other Staff member or the individual concerned.
- The photos of card holders on the ACS and VMS may not be used for any other purposes. The card holders give permission for the photos to be used only for the issuing of an access card.
- Activating of release buttons of any electronic doors or gates will not be permitted and all requests must be directed to the Director: Security Services.
- Access cards can be suspended by the Legal Division of the University on the PeopleSoft system, which will result in all access rights being removed from the card and an exception alarm being triggered on the scanner systems.
- Rules applicable to card holders and Permission Manager Administrators are captured in Annexure A.

6.5 Visitor Management System (VMS)

- Deans and Directors can nominate authorised Staff to apply and approve Visitor access for meetings, workshops, etc. in accordance with the rules applicable to users of the Visitor Management System (see Annexure B).
- Visitors are invited via the UP-Portal Visitor Management System in accordance with the rules applicable to users of the Visitor Management System (Annexure B) and a PIN code will be sent via SMS to the Visitor for access to the University's premises.
- The Visitor will have to present the PIN code as well as proof of identification in order to gain access.

7. Roles and Responsibilities

The Registrar

The Registrar has overall accountability and responsibility for ensuring that all institutional policies are managed responsibly within the University.

The Chief Operating Officer

The Chief Operation Officer will ensure that support and resources are available to the Department of Security Services for the implementation of the Access Control Policy.

The Director Security Services

The Director Security Services is responsible for the implementation, enforcing and communication of the Access Control Policy, ensuring the security of Students, Staff, Contractors and Visitors to all University Campuses and other premises, and adopting a proactive approach to minimise crime and security incidents and their effects on the University, Staff Students, Contractors and Visitors.

The Department Information Technology

The Department Information Technology Services is responsible for the integration of the Staff members records from PeopleSoft to the VMS and ACS and manages business rules, database management and system upgrades. In addition, the installation and maintenance of the network communication and licencing of scanning devices form part of this responsibility.

The Department Security Services

The Department Security Services is responsible to manage access rights, user profiles, access group and time pattern set-up on the ACS and VMS.

The Department Facilities Management

The Department Facilities Management is responsible for the installation and maintenance and repair of hardware (readers, boom gates etc).

The Student Service Centre

The Student Service Centre is responsible for the issuing of UP access cards.

Staff, Students, Visitors and Contractors

Staff, Students, Visitors and Contractors must adhere to the access control policy, paying particular attention to the safekeeping and responsible usage of the UP-access card.

8. Associated documents

- General rules and regulations for the dual verification access control system for all campuses and residences
  - Security Policy
  - Traffic and Parking Management Policy and Rules
  - IT User Access Policy
  - Rules applicable on access card users and Permission Manager Administrators
  - Rules applicable on users of the Visitor Management System

9. Policy life cycle

The access control policy should be reviewed every three years or sooner if deemed necessary. This policy remains in force until an amended policy is approved.

10. Document metadata

Document number:	*Rt 205/22*
Document version:	*Rt 205/22 is the newly approved version replacing Rt 319/18 (final)*
Document approval authority:	*Executive*
Document approval date:	*24 May 2022*
Document owner:	*Director: Security Services*
Document author(s):	
Next review date:	*24 May 2025*
Visibility: Display on staff intranet Display on student intranet Display on public web	 √ √