UNIVERSITY
OF
JOHANNESBURG

POLICY ON ISSUING ACCESS CREDENTIALS FOR THE UNIVERSITY AND AMENDMENTS

Division/Unit/Department	Protection Services
Policy Owner	Chief Operating Officer
Responsible Division	Operations
Date of Initial Approval	21 June 2011
Approved by	Academic Administration Managers
Approval dates of revision and amendments	2021
Date of Approval	23 November 2021
Approved by	Management Executive Committee (MEC)
Next Review date	2026
Platform to be published on	Intranet

CONTENTS

1. INTROCUCTION 3

2. PURPOSE AND SCOPE 3

3. PRINCIPLES AND VALUES 3

4. CATEGORIES OF ACCESS CREDENTIALS 3

5. DE-ACTIVATION OF CREDENTIALS 4

6. LOST, WORN OR DEFECTIVE CREDENTIALS 5

7. NUMBER OF CREDENTIALS PER PERSON 5

8. ACCESS LEVELS 5

POLICY ON ISSUING ACCESS CARDS FOR THE UNIVERSITY

1. INTRODUCTION

The provision of a safe and secure environment is a strategic enabler for the core University activities of teaching, learning and knowledge production. Implementing effective access control measures enables the University's Protection Services Department to identify, prevent and detect safety and security-related risks, threats, or breaches on its campuses.

2. PURPOSE AND SCOPE

The purpose of this policy is to:

2.1 Establish a clear set of directives regarding the issuing and control of access credentials–to designated groups within the University Community.

2.2 Ensure standardization of all matters pertaining to the issuing of access credentials.

2.3 Identify responsible divisions and role-players.

2.4 This policy has institution-wide application.

3. PRINCIPLES AND VALUES

The Policy reflects the tenets of risk management regarding the issuing and control of access credentials and includes the following:

3.1 Generally accepted principles of good governance.

3.2 Uniformity of processes and usage across all campuses.

3.3 Explicit identification of responsible divisions and role-players.

3.4 Accountability.

This policy must be read in line with the following policies and regulations:

a) UJ Vision, Mission and Values.

b) All relevant internal Policies, Regulations, Guidelines, Contracts.

c) All relevant regulations such as PAIA etc.

d) All relevant Protection Service Policies.

4. CATEGORIES OF ACCESS CREDENTIALS

The following categories of access credentials are issued:

4.1 Access credentials for all employees active on the official Human Resources (HR) information system.

4.2 Access credentials for all students registered on the official student information system for the current academic year.

4.3 Access credentials are also issued to the following categories, as and when the need arises:

4.3.1 Council members.

4.3.2 Approved service providers / Contractors.

4.3.3 Approved library users.

4.3.4 Registered alumni.

4.3.5 Approved/pre-arranged visitors e.g., students attending short courses offered by external individuals/institutions.

4.3.6 Gym.

4.4 Category 5.3 credentials are issued under the following conditions:

4.4.1 Details of all credentials holders are captured on the relevant official information system.

4.4.2 All credentials display a photograph of the person, staff, or student number.

4.4.3 All credentials indicate the category type.

4.5 Requests for category 4.3 credentials are done in writing and approved by the Senior Academic Administration Officer Host Department or Faculty, then forwarded to the Systems Administrator: Access Cards at Protection Service on the APK campus for processing/issuing of credentials.

4.6 Access permit.

An access permit is a document allowing the holder access to UJ premises for a specific reason and definite period. It is issued to contractors who are not UJ employees nor student, to enable them to access UJ premises to perform work. Among other the permit needs to reflect the Company name, the personal details of the contractor such surname, ID and the contact details of the responsible person with UJ.

These permits are issued by Central Technical Services and approved by Occupational Health and safety. Each permit will be accompanied by a copy of the ID document of the employee, the period in which the permit is valid will be indicated and the full biographical detail of the employee is to be included.

5. DE-ACTIVATION OF CREDENTIALS

5.1 Access credentials issued under 5.1 are de-activated when an employee leaves the service of the University. This is done by entering an end date on the official HR- information system. All physical access credentials are handed over to the relevant person for the department and this is usually handed over to HR – these intern needs to be handed over to Protection Services to discard of.

5.2 Access credentials issued under 5.2 are only active for the current academic year or until a cancellation date is recorded on the official student information system by the faculty administration.

5.3 Access credentials issued under 5.3 are only active up to the end date as entered on the relevant information system.

6. LOST, WORN OR DEFECTIVE CREDENTIALS

5.4 A fee, as determined annually by the Finance Committee and published in the Fees Brochure is charged for all lost access credentials.

6.1 Worn or defective access credentials are replaced free of charge at the discretion of the Senior Manager: Systems and Access Control when the worn or defective access credentials is handed in at the Protection Services office. These worn or defective physical access credentials are kept for one calendar year for auditing purposes and then destroyed by Protection Services.

6.2 Worn or defective access credentials are replaced under the following conditions:

- Lost Access Credentials due to negligence will be charged @ 100% rate as determined by the finance committee.
- Worn / Damaged credentials within a period of a year will be charged at 75% rate of the normal charge as determined by the finance committee.
- Worn / Damaged credentials within a period of 2 years will be charged at 50% rate of the normal charge as determined by the finance committee.
- Worn / Damaged credentials within a period of 3 years and above will be charged at 0% rate of the normal charge as determined by the finance committee.

6.3 Defective access credentials handed in at the Protection Services office. These worn or defective access credentials are kept for one calendar year for auditing purposes and then destroyed by Protection Services.

7. NUMBER OF CREDENTIALS PER PERSON.

Users will be issued with either one or two credentials in instances where the user is both staff and student or alumni.

8. ACCESS LEVELS.

Access levels are determined by the Senior Director Protection Services.