**INTEGRATED MANAGEMENT SYSTEM**

(ISO 9001:2015, ISO 14001:2015, ISO 45001:2018)

**UPIK Security Policy**

**IMS/HSE/PROC06.28v0**

March, 2024

Amendment record
This Policy is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual additions or omissions is given below:

|  |  |  |  |
| --- | --- | --- | --- |
| Page No. | Context | Revision | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Approval

The signatures below certify that this policy has been reviewed and accepted and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Name** | **Signature** | **Position** | **Date** |
| Prepared By | Sergius Katushabe |  | Lead Implementor  | 27/03/2024 |
| Reviewed By | Bessie Nandutu |  | Records Officer | 4/4/2024 |
| Approved By | Bernard Ongodia |  | Principal | 4/4/2024 |

**1. PURPOSE**

The purpose of this document is to outline UPIK's responsibilities in relation to the: maintenance of a safe and secure physical environment for the UPIK population; and protection of UPIK property.

**2. SCOPE**

This policy covers physical security as it relates to the UPIK population and UPIK property.

**EXCEPTIONS**

The definitions described under Section 4 and the scope described under Section 5.1 of this policy limit the policy's applicability. Matters relating to Information Security and security of research materials are covered under other UPIK policies. The policy does not govern the behaviour of non-UPIK staff that occupy leased space owned by UPIK. The policy does not cover property security at locations that UPIK does not own or control.

**3. REFERENCES**

ISO 9001:2015 QMS

ISO 14001:2015 EMS

ISO 45001:2018 OHSM

PROCEDURE FOR EMERGENCY PREPAREDNESS AND RESPONSE

**4. DEFINITIONS**

**Contractor**

A company, organisation, or person that has a formal contract (other than an employee contract) with the UPIK to carry out work on or in UPIK Property.

**Physical Security**

That which is done to facilitate the existence of a stable, relatively predictable environment in which: the UPIK population is able to pursue UPIK's business without disruption or harm and without fear of disturbance or injury; and loss or destruction of UPIK property arising from unauthorized access, theft, or malicious or accidental acts is minimized.

**Restricted Area**

Any area of the UPIK that is only accessible to authorised persons from the UPIK population at particular times.

**Security Agency Staff**

Persons employed by a Security company that have been hired to provide security or patrol services on UPIK Property.

**Security Incident**

Any act, omission, circumstance, or occurrence which directly or indirectly adversely affects, or is likely to adversely affect, the: safety and security of the UPIK population; and availability and utility of UPIK property.

**Security Staff**

A member of the UPIK staff employed to provide all or part of the security services provided by the Security Office.

**UPIK Business**

Any approved work related to employment at UPIK or in connection with the official functions of UPIK.

**UPIK Population**

Staff, Students, UPIK Associates, Visitors and Contractors.

**UPIK Property**

Any property within UPIK's control that is used for, or to support, UPIK business.

**Visitor**

A person invited to the campus by a UPIK member or an enrolled student.

**5. POLICY STATEMENT**

**5.1 Scope**

This policy determines the roles, responsibilities or requirements for the following:

i. Security Staff

ii. Personal Security

iii. Building Security

iv. Property Security

v. Physical and Electronic Key Control

vi. Incident Reporting

vii. Vehicular Movements

viii. UPIK Population Identification

ix. Physical Transfers of Cash

x. Purchase of Security Systems, Products and Services

**5.2 Security Staff**

The primary role of a Security Staff is to observe, report and monitor anti-social behaviour and any issues of safety and security in relation to UPIK population or UPIK Property. Security Staff do not have Police powers, the authority of state government agencies or the protection offered to these groups under the relevant Acts. However, Security Staff are authorised to uphold the relevant Land and Traffic By-Laws. Security Agency Staff are covered by this policy.

**5.3 Personal Security**

Staff and Students will make themselves aware of all UPIK security procedures relating to their activities and will discharge those responsibilities to the best of their abilities. Staff and Students shall take reasonable precautions to protect their own personal safety and the safety of their personal belongings whilst on UPIK Property. The Security Office will provide information to assist staff and students in protecting their personal safety and belongings.

**5.4 Building Security**

Access to UPIK facilities is a privilege and must be controlled to protect the security of UPIK assets. Access privileges to facilities are temporary and may be revoked immediately. The Security Office is responsible for determining and implementing adequate perimeter security systems for all buildings on UPIK Property.

The Security Office is responsible for securing the external perimeter of all UPIK buildings at UPIK. At other locations, the relevant delegate, is responsible for securing the external perimeter of all buildings under their jurisdiction. Building occupants shall ensure that unauthorised access to rooms and buildings under their control is prevented in line with the relevant Security procedures. All physical access to UPIK Property shall be controlled by police, with access to such property granted on the basis of identified need for members of the UPIK Population. The Security Office shall prepare and monitor this policy.

**5.5 Property Security**

Building occupants are responsible for securing all UPIK property located within areas under their control (e.g. equipment, materials, records, furniture) to prevent undetected access, removal or damage.

**5.6 Physical and Electronic Key Control**

The control and issue of keys, access devices and locking mechanisms for use by UPIK staff, students and other authorised persons shall be managed to minimise the risk of unauthorised access. All Master and Service Keys shall be managed centrally by estates manager.

**5.7 Incident Reporting**

All security incidents are to be reported to the Security Office.

**5.8 Vehicular Movements**

Vehicle movements on UPIK Property will be permitted in accordance with Traffic By-Laws. Vehicle movements will be restricted in and near pedestrian precincts of the campus. Speed limit on campus shall be 20km/hour.

Unless authorized, no commercial motorcycles are allowed beyond the official UPIK gate for any reason whatsoever. Those authorized can only be allowed to their destination strictly for the purpose against which they have been authorized.

**5.9 UPIK Population Identification**

Staff and students must produce their UPIK identification card upon request by an authorised person. Staff and students must wear their identification card at all times when physically located at, or while visiting, a restricted area. Contractors and Security Agency staff working within UPIK Property shall sign in at the Security Office (UPIK Campus) or main reception area (all other locations) on arrival each day, obtain and display a temporary identification badge for the duration of their stay, and return the badge and any keys to the Security Office or relevant reception area upon signing out.

**5.10 Purchase and Installation of Security Systems, Products or Services**

All matters relating to the purchase or installation of Security Systems, Products, or Services for use on UPIK Property by Staff shall, in the first instance, be referred to the HSE officer and the Security Person on campus on approval by the Principal. The Security person on campus shall ensure that all Security Systems, Products and Services comply with the prevailing standards prior to approval for their procurement.