



**JARAMOGI OGINGA ODINGA UNIVERSITY
OF SCIENCE AND TECHNOLOGY**

SECURITY POLICY AND PROCEDURE MANUAL

May 2016

Jaramogi Oginga Odinga University of Science and Technology

SECURITY POLICY AND PROCEDURE MANUAL

2016

© Copyright JOOUST 2016

This policy was written and produced by Jaramogi Oginga Odinga University of Science and Technology

P.O. Box 210-40601 Bondo, Kenya

Telephone: + 254 - 57 2501804 / 2058000

Fax: + 254 - 572523851

Email: vc@jooust.ac.ke

Website: <http://www.jooust.ac.ke>

Policy Title: Security Policy and Procedure Manual

Policy Theme: To ensure the provision of a safe and secure environment for Teaching, Research and Learning through enhanced security at the University.

Policy Contact: Chief Security Officer

Approval Authority: The Council

Category: Security Services

Reference No: JOOUST/VC/LO/P/26

Status: Approved By Council
26th May 2016
Minute 7/20/05/2016

Commencement Date: 26th May 2016

Signed:



Vice-Chancellor, Secretary to Council
Prof. S. G. Agong'

3/2/2017

Date



Chairman of Council
Dr. B. J. Mwandotto

3/2/2017

Date

TABLE OF CONTENTS

Contents

LIST OF ABBREVIATIONS AND ACRONYMS	7
POLICY FRAMEWORK	8
1 SECURITY POLICY	9
1.1 Policy Statement.....	9
1.2 Responsibilities	9
1.3 Roles	9
2 CRIME PREVENTION.....	11
2.1 Security Awareness	11
2.2 Incident Reporting	12
2.3 Crime Investigation.....	12
3 ACCESS CONTROL	12
4 CROWD CONTROL, WEEKEND FUNCTIONS/EVENTS, STUDENT & OUTREACH ACTIVITIES	13
4.1 Procedure: Out of Hours Access	13
4.2 Procedure : Handling of Demonstration/Riots	13
4.3 Procedure : Students Elections.....	13
5 CONTROL OF KEYS	13
5.1 Procedure: Request for keys	13
5.2 Procedure: Loss of keys	13
5.3 Procedure: Hand over of keys	13
5.4 Procedure: Transport Vehicle Keys.....	14
6 EQUIPMENT PROTECTION	14
6.1 Security of Equipment	14
6.2 Security Hardware	14
6.3 Headed Paper and Stationary.....	14
6.4 Confidential Waste	14
7 ASSET PROTECTION	15
7.1 Control of Cash	15
7.2 Security in the Office	15
7.3 Personal Security	15
7.4 Drugs and Illegal Substances	16
7.5 Property lost and found.....	16
7.6 Students.....	16
7.7 University Vehicles	16
8 VEHICLES PARKING ARRANGEMENT.....	17
8.1 Reserved Parking	17
8.2 Staff Parking.....	17
8.3 Residential Staff Parking	17
8.4 Motorcycles and bicycles.....	17
9 USE OF CLOSED CIRCUIT TELEVISION	17
10 FIRE/EMERGENCY RESPONSE TRAINING/DRILLS	17

11 SECURITY RISK ASSESSMENT 18
12 REVIEW OF POLICY 18

PREAMBLE

Jaramogi Oginga Odinga University of Science and Technology will endeavor to ensure, as far as reasonably practical, the personal safety and security of all students, staff and visitors to the University and all university controlled buildings.

The responsibility for security and personal safety rests with all persons who study, work or reside in or who visit the university.

Unless otherwise specified, reference to Jaramogi Oginga Odinga University of Science and Technology in the document shall cover all campuses, learning centers and associated buildings.

This policy covers all aspects of security pertaining to the University

LIST OF ABBREVIATIONS AND ACRONYMS

AV	Audio-Visual
CCTV	Closed Circuit Television
IT	Information Technology
ICT	Information Communication Technology
JOOUST	Jaramogi Oginga Odinga University of Science and Technology
LAN	Local Area Network
SAJOOUST	Student's Association Jaramogi Oginga Odinga University of Science and Technology

POLICY FRAMEWORK

This policy shall be read and enforced alongside:

Laws of Kenya being the Evidence Act; Criminal Procedure Code; the Penal code and any other relevant Act as will be amended from time to time

Universities Act No. 42 of 2012

Jaramogi Oginga Odinga University of Science and Technology:

- Charter 2013
- Statutes 2013
- Code of Ethical Principles and Conduct 2013
- Rules & Regulations Governing the Organization, Conduct and Discipline of Students 2013
- ICT Policy 2013
- Risk Management Policy 2013
- Anti-Corruption Policy

Terms of Reference:

- i. To review security policy, strategy and procedures;
- ii. To monitor the effectiveness and efficiency of security operations and procedures to ensure their continued effectiveness;
- iii. To bench mark the delivery of an efficient and effective security service with best practice and
- iv. To review Staffing provisions for security operations in the university.

1.3.5 Vice-Chancellor

To promote and maintain good order in the university

1.3.6 Chief Security Officer

- a) Oversee security operations in close consultations with the Vice-Chancellor ;
- b) Implement security strategy, policies and procedures;
- c) Manage intruder alarm systems and CCTV systems effectively and efficiently;
- d) Investigate crime, breaches in security and non academic student disciplinary matters;
- e) Organize regular fire and evacuation drills;
- f) Provide professional, impartial and up-to date advice;
- g) Coordinate and integrate any contracted security services into the university security operations in an efficient and cost effective manner;
- h) Liaise with the police, emergency services and local authorities as directed by the Vice-Chancellor and;
- i) Any other duty as directed by the Vice-Chancellor

1.3.7 Deans, Directors and Heads of Departments

Have a key role in promoting security within areas under their jurisdiction. Whilst it is recognized that the Deans, Directors and Heads of Departments may wish to delegate responsibility to nominated individuals in their Schools, Centers, Departments, the overall responsibility for security matters will remain with the Dean and Head of Department to:

- a. Ensure that all their staff have access to and are familiar with security policy, paying particular attention to those issues which are directly relevant to the activity of their School /Department;
- b. Ensure that all members of staff and students in their respective schools/departments understand and discharge their security responsibilities, including the display of University identity card and have respect for University property;
- c. Safeguard any ICT equipment including network infrastructure
- d. Liaise with the Head of Security on any security matters;
- e. Control access to their School/Departmental areas by approving the issue of the keys and by authorizing staff to have out of hours access only as deemed necessary;
- f. Ensure that their staff surrender to the department their University identity card and any issued keys on their last day of work;
- g. Notify the security team of any security risk (including purchase of expensive equipment) for advice on any additional security or protection; and
- h. Ensure that all students surrender to the Academic Registrar's Office. their Student Identity Card on collection of their certificates or on suspension or expulsion

1.3.8 Security Staff

Security duties include:

- a. patrol of perimeter areas to deter trespass,
- b. regular patrol of building vicinity to deter trespass or unauthorized removals of assets,
- c. daily locking/unlocking procedures of premises ,
- d. access controls especially for events held outside events held out of normal working hours,

- e. Safeguard of Local Area Network Infrastructure in common areas such as Assembly Hall, lecture rooms and Wi-Fi access points,
- f. Reporting incidents to supervisor,
- g. Logging of incidents in designated Incident Books,
- h. Crowd control, and
- i. Checking all vehicles entering and leaving the university premises.

1.3.9 Staff

All staff must:

- a. Ensure that they are familiar with and adhere to procedures,
- b. Co-operate with requests from security team, especially in emerging or evacuation situations and in relation to security procedures,
- c. Carry their University identity cards at all times, and
- d. Report all suspected or real activities, of a criminal nature or any seemingly suspicious activity immediately to the security staff.

1.3.10 Students

All students must:

- a. Look after and take care of University facilities and to give due consideration to security issues,
- b. Carry their University identity cards at all times and produce it on demand,
- c. Adhere to security procedures designed to protect University property in particular regulations governing access to computer laboratories, library or areas with equipment for public use,
- d. Co-operate with requests from security team in emergency or evacuation situations, and
- e. Report all suspected or real activities, of a criminal nature or any seemingly suspicious activity immediately to the security staff.

1.3.11 Visitors

All visitors must:

- a. Respect University assets and property
- b. Adhere to security procedures designed to protect University property
- c. Wear their visitors badge at all times
- d. Adhere to instructions and guidelines from the security team or from their host Department, particularly in emergency situations and
- e. Conduct themselves in an orderly manner while in the University

1.3.12 Contractors/Suppliers/Partners

All contractors/ suppliers/partners who make use of and/or work on university property are required to:

- a. Seek approval from the relevant authorities in order to do so,
- b. Give due consideration to personnel security and safety issues whilst on university premises,
- c. Adhere to instructions and guidelines from the security department, and
- d. Carry their gate pass and produce it on demand

2 CRIME PREVENTION

2.1 Security Awareness

Proactive crime prevention and security awareness will help to ensure a safe, secure environment, enabling work and study to continue with the minimum amount of disturbance. Staff and students should make every effort to counter the threat of crime.

2.1.1 Procedure: Crime Prevention and security awareness

- a. All suspicious activity should be immediately reported to the security office,
- b. Personal valuables should be locked away or placed out of sight or kept on the person and personal property should never be left unattended,
- c. All windows in ground floor offices must be closed and secured on departure where locks are fitted,
- d. Laptops and other portable IT/Audio Visual equipment should be locked out of sight when not in use, and
- e. Security officers to make external patrol of the buildings to identify security risks, monitor public safety and act as deterrent against crime.

2.2 Incident Reporting

It is the responsibility of all staff and students of the University to report all activities, suspected or real, of a criminal nature. Incident reporting is crucial to the identification of patterns of criminal activity. It permits investigation and recommendation to be made to prevent a recurrence. Comprehensive reporting of incidents throughout the University ensures that adequate resources are provided to combat that crime. Success in the fight against crime is greatly enhanced by fast, efficient and detailed reporting.

2.2.1 Procedure: Reporting of security incident

- a. All incidents of a security nature should be reported in the first instance to the Chief Security Officer or Supervisor on Duty and
- b. Criminal offences committed by students should only be reported to the police by Chief Security Officer in line with student regulations and after consultations with the Vice-Chancellor.

2.3 Crime Investigation

All crimes that occur on University premises will be investigated so as to prevent re-occurrence and aid crime prevention. The Chief Security Officer or other members of the security team as delegated will carry out internal investigations of the security related incident, produce written reports for circulation where necessary and provide follow up crime prevention advice.

3 ACCESS CONTROL

- 3.1 All staff and students are issued with JOOUST cards which are used as identity card. Students are required to carry their cards with them at all times and to produce them on demand. Staff is also required to carry their cards at all times Whilst on University premises;
- 3.2 Visitors and ad-hoc contractors will-be issued with a visitor's pass at the point of entry after giving their full particulars and should wear these passes, throughout their visit to the University. The members of staff responsible for the visitor/contractor should ensure they sign the visitors pass before it is returned upon leaving the University;
- 3.3 Contractors who will be on site for more than a week will be issued with a University 'contractor' card to allow them access to the building they are working in. Contractor identity cards must be displayed at all times whilst on University premises and produce them on demand;
- 3.4 All vehicles entering/leaving the University shall be subjected to security checks; and
- 3.5 Key offices will be restricted and accessed only through personnel security guards and or use of appropriate scanning devices.

4 CROWD CONTROL, WEEKEND FUNCTIONS/EVENTS, STUDENT & OUTREACH ACTIVITIES

4.1 Procedure: Out of Hours Access

- a. The use of University premises during weekdays, weekends or out of hours is restricted and those wishing to organize an event should get authority from the relevant authority and
- b. Staff who require to work in their offices outside normal University working hours need to notify the security office.

4.2 Procedure : Handling of Demonstration/Riots

The Security Department shall ensure that;

- a. Early warning mechanisms are in place to forestall the occurrence of riots,
- b. Grievances, unlawful meetings, inciting information and unruly behavior is reported to the relevant authorities within the shortest possible time,
- c. In the event of riots/demonstrations:
 - i. Security personnel are assigned to gather intelligence to identify the perpetrators,
 - ii. Adequate measures are in place to protect University staff and students,
 - iii. Vital installations and property are protected,
 - iv. Traffic within the university is diverted to safer routes to avoid damage and injury,
 - v. Other Government Security agencies are contacted, if necessary, after consultations with the Vice-Chancellor,
 - vi. The injured are evacuated for medical attention as soon as possible, and
 - vii. University property is protected against looters during and after.

4.3 Procedure : Students Elections

- a. Security arrangements prior, during and after students elections must be agreed upon between the SAJOUST Electorate Board and the Chief Security Officer ,
- b. Adequate resources and provisions be made well in advance,
- c. Heightened state of vigilance should be maintained, and
- d. Control procedures should be in place to handle disruptions and emergency situations.

5 CONTROL OF KEYS

The caretaker to liaise with Departmental Administrators to keep a record of all keys issued locally and ensure staff return keys when they move offices or leave University employment University. It is the responsibility of all individuals who are issued with keys to ensure their safe keeping at all times and report any loss immediately to security staff.

5.1 Procedure: Request for keys

Any request made by the security officers for keys or access to keys must be granted in emergency situations.

5.2 Procedure: Loss of keys

- a. All keys lost must be reported immediately to the security office and will be the subject of an investigation,
- b. Lock should be replaced immediately keys are reported as lost as a precautionary measure, and
- c. The replacement expense should be charged to the person responsible

5.3 Procedure: Hand over of keys

Persons leaving the University or transferring to another department are required to hand over their keys to the security office.

5.4 Procedure: Transport Vehicle Keys

All University transport vehicle keys should

- a. Have a designated depository and
- b. Be signed in and out at all times

6 EQUIPMENT PROTECTION

6.1 Security of Equipment

The safekeeping of all property will help to ensure that every piece of equipment is available for use at all times. Students and staff are to make all possible efforts to ensure that all equipment are protected from theft or damage.

6.1.1 Procedure: Security of Equipment

All computers and other valuable equipment should be secured irrespective of whether it belongs to the department or not i.e. shared telephone or Local Area Networks. Equipment used in the department and facilities must be managed to reduce the risk of the equipment being damaged, stolen or accessed by unauthorized persons:

- a. Portable IT equipment and other valuable equipment must be always be secured,
- b. Equipment should be labeled using appropriate the university identification code and an inventory of the same kept,
- c. Suspected theft of equipment should be reported promptly to both the Chief Security Officer and the Finance Officer, and
- d. Heads of Departments must maintain inventories for all plant, equipment and furniture in their departments or under their respective jurisdiction.

6.2 Security Hardware

Installation of CCTV, intruder alarms or access control systems in University premises or buildings will be undertaken under the supervision of the Chief of Security. Advice on the technical specifications and detailed functionality, where appropriate, will be sought from the relevant departments with such specialized expertise. The Chief of Security will advise on broad functionality of equipment, installers and security response.

6.3 Headed Paper and Stationery

Pre-printed headed paper and other stationery displaying University logo, staff names, telephone numbers, must be treated carefully to avoid fraudulent use.

6.3.1 Procedure: Handling Headed Paper and Stationery

- a. Headed paper, order forms, compliment slips should be locked away when not in use.
- b. Old or unwanted headed paper must be disposed of correctly by shredding or using a confidential waste disposal system.

6.4 Confidential Waste

It is the responsibility of Departments to ensure that confidential waste is collected and disposed of properly.

7 ASSET PROTECTION

Heads of Departments are responsible for maintaining proper security at all times for all buildings, stock, stores, furniture, equipment and cash under their control.

7.1 Control of Cash

7.1.1 Procedure: Handling of cash

- a. Cash from all sources throughout the University should be processed and taken to the Bank under armed escort or by an appointed cash carrying firm,
- b. Any cash held must be retained in a secure safe,
- c. Large sums of money should not be kept in the safe or held within the Departments overnight or during weekends,
- d. All existing safes and new safes acquired should be insured, and
- e. Proper safe keys control measures must be put into place, ensuring appropriate arrangements are in place to cover holidays and absence due to sickness.

7.2 Security in the Office

It is the responsibility of all staff to be aware of and familiar with all procedures that ensures a safe and secure environment for personnel, equipment and documentation in their office areas.

7.2.1 Procedure: Office Security , General

- a. University ID cards should be carried by students and staff at all times on University premises,
- b. Students and staff should be aware of the security office telephone number for gaining assistance and reporting incidents,
- c. Any suspicious behavior should be reported to the security on the emergency number or other means,
- d. Staff working "out of hours "should notify the security officer and contact him if they need assistance and,
- e. Confidential material (hardcopy) is properly secured at all times and soft copies files password protected and or encrypted.

7.2.2 Procedure: Office Security, End of working hours

Staff should ensure that:

- a. Valuables such as laptops are locked away ,
- b. Confidential documents (exam script, research data, personnel files) are locked up and related softcopy files password protected and or encrypted,
- c. All non-essential appliances are switched off/unplugged,
- d. Curtains are drawn and doors closed and locked. Any items on windowsills which hinder drawing of curtains removed and lights turned off,
- e. Intruder alarm system when installed are set, and
- f. Computers switched off or user access password protected when not in use to prevent unauthorized access to information.

7.3 Personal Security

Whilst it is the responsibility of the security team to provide a safe and secure environment, it is the responsibility of all staff and students on University premises to take all reasonable measures to ensure their own personal security.

7.3.1 Procedure: Suspicious behaviour

If a suspicious activity is noticed, notify or get a colleague to notify the security officer on duty immediately. The security staff will direct security response to the area as a matter of urgency and if appropriate, ensure that the police are contacted.

7.3.2 Threatening or Abusive Behavior

If staff or students are faced with threatening or abusive behavior they should report immediately to a security officer after removing themselves from that situation.

7.4 Drugs and Illegal Substances

7.4.1 Procedure: Suspicious handling or use

All suspicions of the handling or use of controlled or illegal substances should be reported to Chief of Security in the first instance for appropriate investigations and consultation with University Authorities may take place.

7.4.2 Procedure: Posing security or safety risk

Schools and Departments which hold substances that might constitute a security or safety risk should contact the Head of Security when appropriate for advice.

7.5 Property lost and found

No items of property or teaching material should be left unattended in teaching rooms.

7.5.1 Procedure: Found property

- a. Undefined found property should be handed into the security office.
- b. When property is handed in the date, time, finder's name, Department and contact details will be recorded.
- c. If the property is not returned to the owner or is left unclaimed for a minimum of one month, the property will be disposed of as the University Authorities may deem fit

7.5.2 Procedure: Claiming property

- a. When a loser claims property, full details will be required i.e. a full description of the item and for certain items, proof of ownership may be requested.
- b. When doubt of ownership exist the Chief Security Officer or the local police, will be asked to arbitrate.

7.6 Students

7.6.1 Student in General

The University does not accept liability for loss and/or damage to students' personal property.

7.6.2 Students in Residence

- a. Students who are residents must strictly adhere to the halls of residence procedures and ensure their personal property is security marked and/or labeled and properly secured.
- b. The University is not liable to losses incurred by students, including through criminal activity whilst in residence.

7.7 University Vehicles

7.7.1 Insurance

All roadworthy vehicles should be comprehensively insured at all times

7.7.2 Work tickets

The work ticket details for every authorized journey for a given vehicle must be duly filled and signed by a designated officer.

7.7.3 Parking

On an authorized journey that entails an overnight stay outside University premises the vehicle should be parked at a Police Station, Chief Camp or any other secure government premise.

8 VEHICLES PARKING ARRANGEMENT

- a. Staff vehicles will be issued with car stickers for ease of identification and to maximize use of the limited available parking space,
- b. All vehicles including motorcycles and bicycles are parked within the universities premises at the owner's risk, and
- c. No vehicles, except those belonging to residential staff and /or the university itself, can be parked overnight or for an extended period of time within university premises without authorization from the relevant authorities. Such unidentifiable vehicles will be clamped and released upon payment of a fine.

8.1 Reserved Parking

The parking bay on the right side as one faces the Administration Block is reserved for designated management staff of the University and clearly demarcated.

8.2 Staff Parking

The parking bay on the left side as one faces the Administration Block is reserved for other members of staff and visitors.

8.3 Residential Staff Parking

Staff who reside within the University are advised to leave their vehicles at the residence parking due to limited parking space.

8.4 Motorcycles and bicycles

- a. The parking area for motorcycles and bicycles will be clearly designated and all staff, students and visitors must observe this,
- b. Motorcycles and or bicycles are prohibited from be ridden along the walkways between buildings due to dangers posed to pedestrians, and
- c. Such vehicles will be clamped and released upon payment of a fine.

9 USE OF CLOSED CIRCUIT TELEVISION

- a. The University shall use CCTV systems around the campus for prevention and detection of criminal activity. Vulnerable areas, public access points and adjacent areas shall be covered.
- b. CCTV images and recordings will be secured in line with the Universities data protection guidelines as stipulated within the JOOUST ICT Policy.
- c. General notices will be displayed regarding the use of surveillance equipment.

10 FIRE/EMERGENCY RESPONSE TRAINING/DRILLS

The Security Department shall:

- a. Signpost clearly emergency exits in all buildings,
- b. Designate assembly and evacuation points in open spaces,
- c. Conduct Fire/Emergency response drills annually,

- d. Train staff and students through workshops and seminars on Fire/Emergency response ,
- e. Liaise with the relevant agencies on fire/emergency response,
- f. Advise the university on matters pertaining to fire/emergency response, and
- g. Develop procedures for handling natural and other disasters.

11 SECURITY RISK ASSESSMENT

The Security Department shall:

- a. Carry out security assessment regularly on a quarterly basis,
- b. Provide findings indicating date of assessment, needs identified, action plan and conclusions, and
- c. Recommend mechanisms to be put in place for monitoring and evaluation of security systems.

12 REVIEW OF POLICY

The Security Policy and underlying procedures will be reviewed regularly by the University Council every three years to ensure its continued application, effectiveness and relevance.