



37/45 KAMPALA ROAD, P.O. BOX 7120, KAMPALA;
Telephone: 256-414-258441/6, 258061, 0312-392000, 0417-302000. Telex: 61069/61344; Fax: 256-414-233818
Web site: www.bou.or.ug E-mail address: info@bou.or.ug

ADVERTISEMENT OF VACANT POSITIONS IN BANK OF UGANDA

Applications are invited from qualified Ugandans to fill the following positions in Bank of Uganda;

1. DEPARTMENT : ADMINISTRATIVE SERVICES
2. JOB REF : ADS5.03
3. JOB TITLE : DRIVER (11- POSITIONS)
4. RANK : DRV III
5. SUPERVISOR : TEAM LEADER TRANSPORT & TRAVEL SERVICES
6. SUPERVISES : NONE
7. JOB PURPOSE:

To safely and efficiently transport Bank staff, guests, and cargo in compliance with national traffic regulations and Bank policies, while ensuring vehicle maintenance, safety, and courteous service at all times.

8. DUTIES AND RESPONSIBILITIES:

- Conduct thorough pre-trip vehicle inspections to prevent avoidable breakdowns and ensure roadworthiness.
- Ensure timely and safe pick-up, transportation, and drop-off of Bank staff, guests, and cargo as scheduled.
- Operate Bank motor vehicles in compliance with the approved transport schedule, national road safety regulations, and the Bank's transport policies.
- Promptly report any vehicle faults, incidents, or accidents in line with Bank procedures.
- Maintain up-to-date motor vehicle logbook record to enable tracking of vehicle movement and fuel usage.
- Maintain cleanliness of the allocated motor vehicle and ensure that all fleet monitoring and security equipment is functional and in good condition.
- Ensure proper security and safety of the Bank vehicle, Bank staff, guests, and cargo.
- Deliver goods or packages in safe condition and to the right address including required documentation.
- Demonstrate professionalism and provide courteous, customer-focused service to all passengers.
- Any other duties allocated by the Bank from time to time.

9. EXPECTED OUTPUTS:

- Well maintained Bank vehicle
- Adequately fueled motor vehicle
- Clean motor vehicle
- Updated motor vehicle logbook and fuel records
- Safety of Bank motor vehicle, staff, guests, and cargo

10. PERSON SPECIFICATIONS:

A. MINIMUM QUALIFICATIONS

- 'O' Level Certificate
- Valid driving permit with classes B&D1.
- Possession of class C and a Certificate in Defensive Driving will be an added advantage

B. EXPERIENCE

- At least five (5) years' experience in driving, (1) one of which must be under driving class D1 in a corporate/company/institution.
- Ability, skills and experience in driving lorries of capacity: 2 rear axle, one front axle, net weight 17 tons and gross weight 29 tonnes will be an added advantage.
- A Clean Driving Record.

C. AGE

Applicants must be 30.0 to 45.0 years as at the close of the advert.

D. COMPETENCIES

i) Technical Competencies

- Basic vehicle maintenance skills
- Good driving skills, including defensive driving skills
- Knowledge of road safety and traffic regulations

ii) Behavioural Competencies

- Transparency and accountability
- Integrity
- Excellence
- Teamwork
- Interpersonal and stakeholder engagement
- Planning and organizing skills
- Self-drive/initiative

11. PHYSICAL DEMANDS OF THE JOB:

Job requires physical strength and good health to withstand long working hours, travel upcountry, sitting for long periods, exposure to different weather conditions and ability to lift medium loads onto and from the car.

12. WORKING CONDITIONS:

- Working outside normal working hours
- Sitting for long periods
- Differing weather conditions
- Long hours of travel

1. DEPARTMENT : SECURITY SERVICES DEPARTMENT
2. JOB REF : SEC4.04
3. JOB TITLE : FORENSICS LABORATORY OFFICER (1- POSITION)
4. RANK : SBOII
5. SUPERVISOR : TEAM LEADER -FORENSICS LABORATORY
6. SUPERVISES : NONE
7. JOB PURPOSE

To ensure security and safety of Bank premises and operations through operational maintenance and utilization of the Bank's forensic laboratory to investigate cyber incidents on the Bank's IT infrastructure.

8. DUTIES AND RESPONSIBILITIES

- Carry out forensic investigations and submit investigation findings reports in accordance with established reporting procedures.
- Operate and maintain the Bank's digital forensic laboratory in a state of readiness by ensuring all tools, equipment, and solutions are up to date, functional, and properly inventoried.
- Create a detailed chain of custody for all evidence collected during forensic investigations.
- Conduct evidence data collection, collation, preservation and analysis using the Bank's Forensic tools in accordance with set guidelines & procedures.
- Perform forensic analysis on computer hardware, software, and operating systems to recover evidential data from damaged equipment or extract information from damaged media.
- Propose enhancements to forensic readiness and digital evidence management and generate forensic intelligence or reports as required by authorized stakeholders.
- Maintain valid support contracts for the tools, solutions and systems in the forensic laboratory.
- Develop annual work activities and attendant budgets for effective investigation operations.
- Budget resources for the effective operations of the Digital Forensic Laboratory and investigations.
- Standardize Laboratory operational procedures in line with policies, best practices and international standards.
- Perform any other duty assigned from time to time.

9. EXPECTED OUTPUTS

- Case Investigation Reports.
- Quarterly forensic laboratory status reports.
- Monthly systems contract management reports.
- Equipment status report.

10. PERSON SPECIFICATION

A. MINIMUM QUALIFICATIONS

- A first-class or second-class (upper) degree in Computer Science, Information Technology, Cyber Security, Digital Forensics, Computer Engineering or Electrical Engineering from a recognized university.
- At least one recognized industry certifications in digital forensics or cyber incident investigations from any of the following bodies: GIAC Network Forensic Analyst (GNFA), GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Examiner (GCFA), GIAC Certified Forensic Analyst (GCF), GIAC Certified Incident Handler (GCIH), GIAC Cyber Incident Leader (GCIL), EC Council Certified Incident Handler (ECIH), EC Council Certified Ethical Hacker (CEH), Offsec Offensive Security Certified Professional (OSCP), PECB Certified Incident Responder (CIR/ eCIR), EC Council Computer Hacking Forensic Investigator (CHFI), Certified Forensic Security Responder (CFSR), EnCase Certified Examiner (EnCE) certification, EnCase Certified eDiscovery Practitioner (EnCEP) certification, Oxygen Forensic Detective, AccessData Certified Examiner (ACE), Magnet Certified Forensic Examiner (MCFE)

B. EXPERIENCE

- Minimum of five (5) years relevant working experience in digital forensics and or cyber incident investigations.
- Working experience in a Security Agency with in-depth understanding of the cyber forensics investigations process is added advantage.

C. AGE

Applicants must be between 30.0 to 40.0 years of age by close of the advertisement.

D. COMPETENCIES

- Digital Forensics science and technology knowledge
- Digital data recovery

- Ethical hacking
- Cyber incident investigation
- Interviewing and interrogation techniques
- Investigation Report writing
- Practical understanding of digital forensic legal regime and the criminal justice system Investigation Report writing
- iv) Behavioral skills
- Time Management
- Problem Solving
- Communication
- Good Listening
- Self-motivation
- Positive Attitude
- Emotional Intelligence
- Conceptual thinking
- Resilience
- Quick decision making
- Analytical & Critical thinking
- Inductive and deductive Reasoning

11. PHYSICAL DEMANDS OF THE JOB

- Work in a lab environment

12. WORKING CONDITIONS

- Work in tense and charged environment during investigations
- Work in a cold environment for extended periods of time.

Applicants must be between 30.0 to 40.0 years of age by close of the advertisement.

D. COMPETENCIES:

i) Technical skills

- Digital Forensics science and technology knowledge
- Digital data recovery
- Ethical hacking
- Cyber incident investigation
- Investigation Report writing
- Digital forensic legal regime and the criminal justice system

ii) Behavioral skills

- Analytical & Critical thinking
- Inductive and deductive Reasoning
- Time Management
- Problem Solving
- Communication
- Good Listening
- Self-motivation
- Positive Attitude
- Quick decision making

11. PHYSICAL DEMANDS OF THE JOB:

- Work in a lab environment.

12. WORKING CONDITIONS:

- Work in tense and charged environment during investigations.
- Working in cold environment for extended periods of time.

1. DEPARTMENT : SECURITY SERVICES DEPARTMENT
2. JOB REF : SEC4.05
3. JOB TITLE : CYBER- CRIME & FORENSICS OFFICER (1-POSITION)
4. RANK : SBOII
5. SUPERVISOR : TEAM LEADER -FORENSICS LABORATORY
6. SUPERVISES : NONE
7. JOB PURPOSE

To ensure security and safety of Bank premises and operations through cyber incident and forensics investigation of incidents on Bank premises and operations.

8. DUTIES AND RESPONSIBILITIES

- Carry out cyber and forensic investigations and submit investigation reports in line with established procedures, including recording and analyzing statements from witnesses, persons of interest, and suspects.
- Collect, preserve, and analyze digital evidence using approved forensic and cyber tools, while ensuring the safe custody of all evidence and adherence to chain of custody procedures.
- Assess cyber threats affecting the financial services industry and provide timely information and recommendations on emerging risks, cyber fraud indicators, and protective measures for the Bank.
- Provide forensic and cyber intelligence upon request, support investigative decisions and advise management on mitigation measures for identified threats.
- Contribute to the development and regular review of digital forensic policies, procedures, and guidelines, and recommend improvements in investigation processes, systems, and evidence management.
- Perform forensic analysis on IT systems by collecting, preserving, and analyzing digital evidence, including recovering data from damaged devices and extracting critical information, in accordance with the Bank's approved tools, guidelines, and procedures.
- Ensure physical security during cyber incident investigations, including controlled access to sensitive environments and proper handling of forensic equipment.
- Conduct staff awareness and sensitization sessions on cybercrime and forensic investigation practices to promote organizational readiness and secure use of ICT resources.
- Develop annual work activities and attendant budgets for effective investigation operations.
- Perform any other duty assigned from time to time

9. EXPECTED OUTPUTS

- Semi-annual and Case Investigation Reports
- Bank, National and International Digital Crime Trend Reports
- Chain of Custody records
- Updated Evidence inventory

10. PERSON SPECIFICATION

A. MINIMUM QUALIFICATIONS

- A first-class or second-class (upper) degree in Computer Science, Information Technology, Cyber Security, Digital Forensics, Computer Engineering, Electrical Engineering from a recognized university.
- At least one recognized industry certifications in digital forensics or cyber incident investigations from any of the following bodies: GIAC Network Forensic Analyst (GNFA), GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Examiner (GCFA), GIAC Certified Forensic Analyst (GCF), GIAC Certified Incident Handler (GCIH), GIAC Cyber Incident Leader (GCIL), EC Council Certified Incident Handler (ECIH), EC Council Certified Ethical Hacker (CEH), Offsec Offensive Security Certified Professional (OSCP), PECB Certified Incident Responder (CIR/ eCIR), EC Council Computer Hacking Forensic Investigator (CHFI), Certified Forensic Security Responder (CFSR), EnCase Certified Examiner (EnCE) certification, EnCase Certified eDiscovery Practitioner (EnCEP) certification, Oxygen Forensic Detective, AccessData Certified Examiner (ACE), Magnet Certified Forensic Examiner (MCFE)

B. EXPERIENCE

- Minimum of five (5) years relevant working experience in digital forensics and or cyber incident investigations.
- Working experience in a Security Agency with in-depth understanding of the cyber forensics investigations process is added advantage.

C. AGE

Applicants must be between 30.0 to 40.0 years of age by close of the advertisement.

D. COMPETENCIES

- Digital Forensics science and technology knowledge
- Digital data recovery

- Ethical hacking
- Cyber incident investigation
- Interviewing and interrogation techniques
- Investigation Report writing
- Practical understanding of digital forensic legal regime and the criminal justice system Investigation Report writing
- iv) Behavioral skills
- Time Management
- Problem Solving
- Communication
- Good Listening
- Self-motivation
- Positive Attitude
- Emotional Intelligence
- Conceptual thinking
- Resilience
- Quick decision making
- Analytical & Critical thinking
- Inductive and deductive Reasoning

11. PHYSICAL DEMANDS OF THE JOB

- Work in a lab environment

12. WORKING CONDITIONS

- Work in tense and charged environment during investigations
- Work in a cold environment for extended periods of time.

1. DEPARTMENT : SECURITY SERVICES DEPARTMENT
2. JOB REF : SEC9.01
3. JOB TITLE : SECURITY ASSISTANT -POOL (29- POSITIONS)
4. RANK : SECURITY ASSISTANT VI
5. SUPERVISOR : TEAM LEADER SECURITY OPERATIONS AND ADMINISTRATION
6. SUPERVISES : NONE
7. JOB PURPOSE

To ensure security and safety of Bank staff, clients, property, premises, operations and activities by carrying out the established security and safety procedures at the duty zones and points.

8. DUTIES AND RESPONSIBILITIES

- Protect the people, operations and assets on Bank premises.
- Carry out searching for persons accessing and exiting Bank premises to prevent unauthorized items from entering or leaving the Bank.
- Process access for authorized visitors, clients and contractors.
- Patrol and surveil the duty bank premises both physically and electronically using CCTV and Access control systems.
- Issue and receive keys for various offices, gates, and bank vehicles to authorized staff.
- Monitor all maintenance activities that take place in the duty area of responsibility.
- Respond to and report immediately to all security and safety emergencies in the BOU premises in accordance with BOU Emergency Response Plan.
- Report all security and safety hazards, threats and incidents in the BOU premises to the supervisor.
- Report faulty security and safety equipment, systems, and tools in the duty area to the supervisor.
- Coordinate effective evacuation of staff and visitors in the duty area to the Emergency Assembly Point
- Carry out emergency rescue for persons during emergencies like lift failure, fire and security incidents.
- Cooperate with and oversee the activities of the outsourced security personnel deployed in the duty area.
- Cooperate with and oversee the activities of the Police security personnel deployed in the duty area.
- Prepare and submit daily, weekly, and monthly security situation reports to the supervisors.
- Man, the Control room whenever always deployed during the shift.
- Review and make Play back of CCTV surveillance systems at Bank premises.
- Retrieve CCTV footage and images of events from the system. Perform any other duties.

9. EXPECTED OUTPUTS

- All staff and clients are received and attended to professionally.
- Staff, clients and customers are professionally guided during emergencies
- Daily security and safety situation reports (comprised of CCTV footage review results, incidents, risk, maintenance activities).
- Monthly duty area performance report (comprised of personnel, incidents, equipment & systems, maintenance activities and visitors).
- Well maintained records of all items existing the bank and incidents in the duty area
- Timely response to and resolution of fire and security emergencies
- Timely incident reports submitted to the supervisor.
- Daily CCTV surveillance system review reports submitted to the supervisor.

10. PERSON SPECIFICATION

A. MINIMUM QUALIFICATIONS

- A diploma in any field of study from a recognized institution.
- Training in Security Services from a National Security Agency or a Recognized/ Licensed Private Security Institution

B. EXPERIENCE

- Must possess Security services working experience of at least three years in a reputable organization
- Experience in operation of electronic security systems and equipment like access control, intrusion detection and CCTV surveillance systems will be an added advantage
- Working experience in the National Security Agencies or Licensed Private Security Agencies shall be an added advantage.

C. AGE

Applicants must be 26.0 to 39.0 years as at close of the advert.

D. COMPETENCIES

i) Technical skills

- Security observation and monitoring skills
- First responder security incident response and handling
- Security risk identification
- Basic electronic security systems operation skills
- Basic firearms handling
- Basic emergency handling equipment operation skills
- Basic computer applications skills
- Good report writing skills in English.

ii) Behavioral skills

- A good command of English
- High Integrity and ethics
- Medium communication
- Polite and courteous
- commitment to duty
- customer orientation
- Good interpersonal skills

11. PHYSICAL DEMANDS OF THE JOB:

Should be able to work for long hours, under pressure, and, with minimal supervision.

12. WORKING CONDITIONS:

Shift work, including weekends, public holidays, and night duty.

13. GENDER REQUIREMENTS

- Ten (10) positions are reserved for female candidates, whose responsibilities will include conducting searches on female staff and

- visitors, in line with best practice search procedures and standards.
- The remaining Nineteen (19) positions are open to all qualified applicants, and selection will take into consideration the need for gender balance and the ability to meet the physical and operational demands of the position, including availability to work extended hours.

1. DEPARTMENT : SECURITY SERVICES DEPARTMENT
2. JOB REF : SEC9.01
3. JOB TITLE : SECURITY ASSISTANT -CONTROL ROOM OPERATIONS (6- POSITIONS)
4. RANK : SECURITY ASSISTANT VI
5. SUPERVISOR : TEAM LEADER SYSTEMS
6. SUPERVISES : NONE
7. Job Purpose:

To ensure security and safety of Bank staff, clients, property, premises, operations and activities by carrying out the established security and safety procedures at the duty zones and points.

8. DUTIES AND RESPONSIBILITIES

- Man, the Control room always during the work shift. Actively monitoring security and safety systems in the Control Room.
- Review and make Play back of CCTV surveillance systems at Bank premises daily.
- Retrieve CCTV footage and images of events from the system upon authorization.
- Modify and update access profiles for authorized staff, visitors, and contractors in the security systems in accordance with established procedures.
- Carry out electronic surveillance of the Bank premises using CCTV and Access control systems to protect people, assets and operations of the Bank.
- Maintain custody of the keys of designated restricted areas.
- Monitor all maintenance activities that take place in the Bank premises using electronic surveillance
- Detect and report security threats, hazards, risks to the supervisor.
- Report and respond immediately to all security and safety emergencies detected in the BOU premises in accordance with BOU Emergency Response Plan and procedures
- Report faulty security and safety equipment, systems, and tools in the duty area to the supervisor
- Participate in the rescue of people during emergencies like lift failure, fire and security incidents.
- Cooperate with and oversee the activities of all security personnel deployed in the Bank premises to ensure adherence to security policies and procedures.
- Prepare and submit daily, weekly, and monthly security situation reports to the supervisors.
- Perform any other duties as assigned.

9. EXPECTED OUTPUTS

- Daily security and safety situation reports (comprised of CCTV footage review results, incidents, risk, maintenance activities)
- Security and Safety System health status reports
- Well maintained inventory of security system and equipment in Control room
- Timely response to and resolution of fire and security emergencies
- Timely incident reports submitted to the supervisor.
- Daily CCTV surveillance system review reports submitted to the supervisor.

10. PERSON SPECIFICATIONS:

A. MINIMUM QUALIFICATIONS:

- A Diploma in ICT from a recognized institution.
- Training in Security Services from a National Security Agency or a Recognized/ Licensed Private Security Institution is an added advantage.

B. EXPERIENCE:

- Must possess working experience in an IT environment of at least three years in a reputable organization.
- Experience in operation or installation of electronic security systems and equipment like access control, intrusion detection and CCTV surveillance systems will be an added advantage.

- Working experience in the National Security Agencies or Licensed Private Security Agencies shall be an added advantage.

C. AGE:

26.0-39.0 years of age at close of the advert.

D. COMPETENCIES:

i. Technical skills

- Security observation and monitoring skills
- First responder security incident response and handling
- Security risk identification
- Basic electronic security systems operation skills
- Basic emergency handling equipment operation skills
- Basic computer applications skills
- Good report writing skills in English.

ii. Behavioral skills

- A good command of English
- High Integrity and ethics
- Medium communication
- Polite and courteous
- commitment to duty
- customer orientation
- Good interpersonal skills
- High Integrity and teamwork

11. PHYSICAL DEMANDS OF THE JOB:

- Should be able to work for long hours, under pressure, and, with minimal supervision.
- Should be physically fit, calm and able to work in emergency situations

12. WORKING CONDITIONS:

- Shift work, including weekends, public holidays, and night duty.

Salary and Benefits for the position are generous and attractive. Please ensure that all required documents are duly attached and must be scanned as a clearly named single document.

Application Submission

Applications should be submitted through the online application link: (<https://forms.office.com/r/BWHcwddqEj>) which is accessible through the careers section of the BOU Website (<https://www.bou.or.ug/bouwebsite/careers/>) Applicants are advised to follow the instructions on the link carefully.

Note

- 1) Applicants **MUST** use the standard BOU Curriculum Vitae form as their Curriculum Vitae format. Candidates that use a CV Format other than that prescribed shall be disqualified. The BOU Curriculum Vitae form is available on the BOU website under the Careers Section.
- 2) Applicants **MUST** append scanned certified copies of academic credentials and professional training certificates to their applications to support their candidature.
- 3) Management reserves the right to disqualify any applicant found to have concealed or falsified information or academic credentials. Only shortlisted candidates will be contacted.

Applications should be submitted NO later than 5:00PM Friday 10 April 2026.