AFRICAN DEVELOPMENT BANK
VACANCY ANNOUNCEMENT N°ADB/13/124

Position title: **INFORMATION SECURITY OFFICER, SECU**	Grade: **PL-5/6**	Position N° : **50000604**	Closing Date: **08 September 2013**
Department/Division: **SECURITY UNIT (SECU)**	Supervisors' Title**: CHIEF INFORMATION SECURITY OFFICER**		

Objectives

This position is located in the Security Unit (SECU). Under the direct supervision of the Chief Information Security Officer (CISO) who reports directly to the Head of the Security Unit, the Senior Information Security officer will be responsible for protecting the Bank's IT resources and information assets based on industry best practices and the Bank's policies and guidance. The candidate will work closely with network, security, and application engineers to collaborate on secure solutions.

Duties and Responsibilities: Under the direct supervision of the Chief Information Security Officer (CISO), the duties and responsibilities are as follows:

- Contribute to the definition and the elaboration of the information security strategy and policies in support of the Bank's business strategy and direction.
- Develop standards, processes, procedures and guidelines that support information security policies.
- Identify and analyze risks through suitable methods approved by the CISO.
- Define and recommend strategies and priority options to mitigate risk to levels acceptable to the Bank.
- Analyze controls and identify significant changes in information risk and report these to the CISO.
- Perform regular vulnerability assessments to evaluate effectiveness of existing controls. Follow-up vulnerability remediation plan, and ensure that non-compliance issues and other variances are resolved in a timely manner.
- Analyze information security issues and apply metrics to measure, monitor, and report on the effectiveness of information security controls and compliance with information security policies.
- Promote accountability by business process owners in managing information security risks.
- Analyze information security risks related to third parties and submit recommendations to the CISO.
- Manage information security projects and manage information security operations.
- Develop business case, budget requirements and terms of reference that support information security programs.
- Participate in the implementation of information security frameworks.
- Define and recommend information security baselines.
- Participate in negotiation relating to information security products or services.
- Develop and deliver effective information security education and awareness to influence culture and behaviour of staff.
- Provide expert advices and recommendations in respect of Information Security.
- Design, elaborate and implement processes for detecting, identifying and analyzing information security related events.
- Recommend response and recovery plans and options to information security related incident.
- Implement periodic testing of response and recovery plans where appropriate, and their execution as required.
- Document appropriately any information security incidents as a basis for subsequent action including forensics when necessary. Produce post- incident reviews and help to identify causes and corrective actions.
- Analyze, formulate, test, optimize and maintain information security recovery plans and procedures in order to assist corporate survival from major processing interruptions.
- Examine complaints or incidents related to information security, investigate and recommend responses and action plans.

Selection Criteria (including desirable skills, knowledge and experience)

- A minimum of a Master's degree in Information Security Engineering, Computer Science, Information Technology or other strongly related discipline.
- Up to date industry certifications (CISSP, CISA, CISM, etc.) covering information security are an added advantage.
- A minimum of four (4) years for the PL6 and five (5) years for the PL5 relevant and demonstrated business environment professional experience in information security implementation/management, or IT.
- Strong understanding of information risk and Security Control Frameworks (ex. COBIT, ISO, ITIL, etc).
- Ability to craft information security standards, procedures, and guidelines.
- Demonstrated understanding of Security Architecture and technologies including Firewalls, IDS/IPS, NAC, SIEM, Content Filtering, vulnerability assessment, authentication systems, etc.
- Excellent analytical, technical and problem solving skills.
- Excellent knowledge of various aspects of information security management in in a range of areas: risk & compliance, security awareness, incident handling, database, network, operating systems, applications development, etc.
- Excellent technical knowledge and experience across multiple platforms and technologies: Windows, Unix, Linux, applications, databases; computer operations, Intranet/Internet, LAN/WAN, etc.
- Good technical knowledge and experience in defining and assessing access and authorization controls within the Bank's critical business applications: SAP. SWIFT, SUMMIT, etc.
- Ability to work within a team and across teams to accomplish common goals.
- Competence in the use of standard Microsoft office applications (Word, Excel, PowerPoint etc).

- Excellent written and verbal communications in English/French with a working knowledge of the other language.

A full background investigation must be completed on the selected candidate

Submitted by: Amir ZAHIR, CHRM.1 Division Manager	**Date**:
Approved by: Joseph O. Badaki, CHRM Director	**Date**:

Only applicants who fully meet the Bank's requirements and are being considered for interview will be contacted. Applicants will only be considered if they submit an online application, and attach a comprehensive Curriculum Vitae (CV). The President, AfDB, reserves the right to appoint a candidate a lower level. The Development Bank is an equal opportunities employer and **female candidates are strongly encouraged to apply**. **http://www.afdb.org**