CIRCULAR No. 316   **14th July, 2023**
OSC Ref. 6272¹⁷

Permanent Secretaries, Heads of Department and Chief Executive Officers are asked to invite applications from suitably qualified officers in their Ministries/Departments/Agencies to fill the following **vacant**, posts in **eGov Jamaica Limited:**

1. **Senior IT Security Engineer (Level 8)** salary range $5,590,000 - $7,520,000 per annum.

2. **Senior Auditor (Level 8),** salary range $5,590,000 - $7,520,000 per annum.

3. **Accounting Clerk/Cashier (Level 4),** salary range $1,550,000 - $2,080,000 per annum.

1. **Senior IT Security Engineer (Level 8)**

Job Purpose

The Senior IT Security Engineer is responsible for the development and implementation of security controls that give effect to the company's IT security policies. The incumbent will participate in the creation and maintenance of security policies, standards, guidelines and procedures, as well as ensures that technical security solutions are optimally configured to protect the Company's data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Key Responsibilities

Management/Administrative
- Contributes to the development of the Department's Operational Work Plans;
- Ensures department projects are managed in accordance with company standards and guidelines as defined by the Project Management Office;
- Participates in cross functional projects to ensure information security requirements are incorporated into system/solution designs and security controls are implemented into these systems/solutions;
- Leads and/or participates in security related projects.

Technical/Professional:
- Participates in the selection and acquisition of additional security solutions and enhancements to the existing security solutions to improve overall security as per the Government of Jamaica procurement guidelines;
- Oversees the configuration and administration of the company's security solutions;
- Executes vulnerability assessments and penetration tests;
- Designs, develops and implements effective security solutions and/or controls to eliminate or otherwise mitigate identified vulnerabilities;
- Develops security administration processes and procedures in accordance with standards, procedures, directives, policies, and regulations;
- Executes penetration testing activities and incident response exercises and ensures lessons learned from incidents are collected in a timely manner and are incorporated into planned reviews;
- Ensures that information systems are assessed regularly for vulnerabilities, and that appropriate solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented;
- Performs security performance testing and reporting, and recommends security solutions in accordance with standards, procedures, directives and policies;
- Monitors system logs, for systems such as firewall, intrusion detection/prevention, and network traffic for unusual or suspicious activity. Interprets activity and makes recommendations for resolution;
- Monitors and assess network security vulnerabilities and threats using various technical and non-technical data and mitigate network security vulnerabilities in response to problems identified in vulnerability reports;

- Performs network security evaluation in regular intervals, estimates risks to the company and recommends remediation activities;
- Conducts research on emerging products, services, protocols, and standards in support of security enhancement and development effort;
- Ensures that all changes to the security solutions comply with approved change Management Policies and Standards;
- Applies security controls in support of the Risk Management Programme;
- Implement threat and vulnerability assessments to identify security risks, and regularly update applicable security controls;
- Participates in the development of Information Security Policies, Standards, supporting guidelines and procedures, ensuring alignment with company objectives and appropriate standards;
- Applies response actions in reaction to security incidents, in accordance with established policies, plans, and procedures;
- Participates in incident response and recovery efforts and prepares security incident reports as required;
- Contributes to the development of Incident Response Plans in accordance with security policies and organizational goals.

Required Knowledge, Skills and Competencies

Technical:
- Hands-on knowledge of firewalls, intrusion detection systems, data encryption, and other industry-standard techniques and practices
- Good technical knowledge of network, PC, and platform operating systems
- Working technical knowledge of current systems software, protocols, and standards
- Strong knowledge of TCP/IP and network administration/protocols.
- Hands-on experience with networking devices
- Good understanding of project management principles
- Good understanding of the requirements of ISO27001
- Ability to deal with diverse and complex issues
- Application & Data Security
- Computer Forensics
- Incident Management
- IT Security Architecture
- Network Operations Security
- Vulnerability Management

Core:
- Excellent oral and written communication skills
- Excellent interpersonal skils
- Excellent problem solving and decision making abilities
- Planning and organizing skills
- Good analytical skills
- Goal and result oriented

Minimum Required Qualification and Experience

- Bachelor's Degree in Engineering or Computer Science.
- Information security certifications such as CCSA, CEH or equivalent (Desirable).
- Minimum of three (3) years' hands-on Information Security experience, supporting complex security environments.
- Minimum of two (2) years experience in Network Management, System Administration or other related disciplines.
- Hands-on experience managing/supporting firewalls, vulnerability assessment solutions, and other security systems.
- Experience in developing security policies/standards, conducting vulnerability and security assessments and designing security controls.
- Experience with SIEM solutions.
- Experience in security incident handling/management.
- Good understanding of the requirements of ISO 27001.
- Ability to deal with diverse and complex issues.

2. Senior Auditor (Level 8)

Job Purpose

The Senior Auditor will participate in the planning of audits to be executed under the supervision of the Department Head – Internal Audit. The incumbent should be able to analyze the company's information security controls in order to identify vulnerabilities in applications, network infrastructure, and operating systems. The Senior Auditor Should also be able to:
- ✓ Conduct audit reviews by consistently reviewing and evaluating the effectiveness and efficiency of the systems of control.
- ✓ Assist in the mentorship of Junior Staff.
- ✓ Must be a good analyst with a critical approach and good knowledge of auditing processes. He /she should have good expertise in risk management and compliance as well as high reliability and strong organizational skills.

Key Responsibilities

Technical / Professional
- Assesses the reliability, integrity, and security of information/operational systems;
- Conducts Security Audits to ensure that current security measures are adequate to protect against threats such as cyber-attacks;
- Ensures compliance with policies, standards, laws, and regulations that could have a significant impact on IS systems or operations;
- Conducts physical audits of computer hardware and software to measure performance levels and detect errors;
- Plans the scope of audits and preparation of audit programmes;
- Obtains, analyzes, and appraises evidentiary data;
- Assesses the adequacy of corrective actions taken by auditees;
- Conducts Risk Assessments;
- Conducts post implementation audits;
- Plans the scope of audits and preparation of audit programmes;
- Appraises the adequacy of corrective actions taken by auditees;
- Ensures the completion and security of working paper files;
- Assists with audit training as needed;
- Prepares written reports;
- Assists in the mentorship of junior Auditors;
- Performs other job enrichment duties.

Required Knowledge, Skills and Competencies

- Excellent oral and written communication skills.
- Knowledge of Government Procurement Policies.
- Good knowledge of the various auditing standards such as ISACA IS Audit and Assurance Standard and Guidelines and Institute of Internal Auditors (IIA) Standards and Guidelines.
- Knowledge of Business Operations.
- Report writing skills.
- Advanced knowledge of best practices in IT controls, data privacy and business (Operational) continuity.
- Excellent Auditing skills

Minimum Required Qualification and Experience

- Bachelor's Degree in Computer Science, Management, or equivalent from an accredited tertiary institution.
- 2-3 years experience directly related to the duties and responsibilities specified.
- Possess Certified Information Systems Auditor (CISA) Certification.
- Applicants who possess CIA Certification would be at an advantage.

3. Accounting Clerk/Cashier (Level 4)

Job Purpose

Under the supervision of the Financial Accountant, the Accounting Clerk / Cashier is responsible for administering and accurately recording all company receipts and disbursements. The incumbent will also perform functions of a Data Entry Operator for the purpose of processing all transactions relating to the updating of monthly accounts.

Key Responsibilities

Technical / Professional
- Prepares receipts for all cash/cheque received by the company;
- Receives, logs, and disburse all cheque payments on a timely basis;
- Prepares lodgement and submit to Financial Accountant for verification;
- Prepares receipt summary on a daily basis;
- Prepares receipts and disbursement data input forms;
- Dispatches cheques to vendors on a timely basis;
- Administer Petty Cash Float;
- Update daily transactions pertaining to Cash book, fixed asset, inventory, accounts receivable and accounts payable;
- Performs Records Management duties;
- Prepares audit schedules.

Required Knowledge, Skills and Competencies

- Good Interpersonal skills
- Good planning and organizing skills
- Team oriented and co-operative
- Good analytical skills
- Customer and quality focus
- Good problem solving skills
- Excellent oral and written communication skills

Minimum Required Qualification and Experience

- ACCA level I or equivalent
- Ability to use Computerized Accounting System
- Proficiency in the use of automated spreadsheets
- 1-2 years experience in a similar environment

Applications accompanied by résumés should be submitted **no later than Thursday, 27th July, 2023 to:**

> **Director**
> **Human Resource Management and Administration**
> **eGov Jamaica Limited**
> **235b Old Hope Road**
> **Kingston 6**

> **E-mail: recruitment@egovja.com**

Please note that only shortlisted applicants will be contacted.

Please ensure that a copy of this circular is placed at a strategic position on the Notice Board of the Ministry/Department/Agency and brought to the attention of all eligible officers.

Merle I. Tam (Mrs.)
for Chief Personnel Officer