The Students' Loan Bureau (SLB) invites applications from suitably qualified persons for the following position:

Network/Security Administrator (Level 8)

The incumbent is accountable for the optimal performance of the Technology Networks in order that SLB achieves its Mission, Vision and Major Targets in a sustainable manner.

Responsibilities & Duties

Planning

1. Contribute to the development of the Corporate Services Division's annual strategic planning process, resulting in the division's cascaded strategic plan and scorecard.
2. Update, in conjunction with direct supervisor, own Job Accountability, ensuring alignment to the Bureau's cascaded strategic plan and scorecard.
3. Develop, in conjunction with direct supervisor, own individual development plan arising from the performance review process.

Execution

4. Provides technical support to all users of the various systems / applications in order to enable timely completion of tasks, ensuring that issues are resolved promptly and efficiently.
5. Troubleshoots and resolves end-users problems and ensures correct operation of personal computers, ensuring that all hardware and software are functioning properly.
6. Installs and maintains new communications and computer equipment, ensuring that all equipment is properly set up and configured.
7. Implements systems modifications required, with appropriate advice to and interaction with relevant department, ensuring that modifications are properly implemented and tested.
8. Trains users in the workings of the IT systems, standards to be observed and the proper use of hardware and software, ensuring that users fully understand how to use the systems.
9. Provides system backups and recovery as scheduled or as requested, ensuring that all data is properly backed up and can be recovered in case of a system failure.
10. Develop, implement, test and maintain systems disaster plans, ensuring that disaster plans are properly developed and tested.
11. Monitors systems and usage of systems to ensure efficiency, ensuring that systems are operating efficiently and identifying areas for improvement.
12. Implement IT security controls, risk assessment framework, and program that align to regulatory requirements, ensuring documented and sustainable compliance that aligns and advances the organization business objectives.
13. Evaluate risks and develops security standards, procedures, and controls to manage risks, ensuring compliance with industry standards and best practices.

14. Implement processes, such as GRC (governance, risk and compliance), to automate and continuously monitor information security controls, exceptions, risks, testing, ensuring the organization's security controls are always up to date.
15. Develop reporting metrics, dashboards, and evidence artifacts, ensuring they accurately reflect the effectiveness of security controls and provide valuable insights to stakeholders.
16. Update security controls and provide support to all stakeholders on security controls covering internal assessments, regulations, protecting Personally Identifying Information (PII) data, and Payment Card Industry Data Security Standards (PCI DSS), ensuring all security controls meet the relevant standards and regulations.
17. Perform and investigate internal and external information security risk and exceptions assessments, assessing incidents, vulnerability management, scans, patching status, secure baselines, penetration test result, phishing, and social engineering tests and attacks, ensuring any potential security risks are identified and addressed in a timely manner.
18. Document and report control failures and gaps to stakeholders, ensuring all stakeholders are aware of any security risks and necessary remediation activities.
19. Provide remediation guidance and prepare management reports to track remediation activities, ensuring all necessary steps are taken to address any security issues.
20. Assist other staff in the management and oversight of security program functions, ensuring all staff members are knowledgeable and up to date on security policies and procedures.
21. Train, guide, and act as a resource on security assessment functions to other departments within the College, ensuring a culture of security awareness and compliance is maintained throughout the organization.

Monitoring and Reporting

22. Contribute to the preparation of the Technology Division's monthly performance report in the scorecard format, then attend the monthly divisional strategy review meeting in discussing performance issues, ensuring there are diagnoses and corrective actions for any performance variances.

Qualifications and Experience

- ✓ First Degree in Information Technology.
- ✓ Certificate in Network and Security Administration.
- ✓ Three (3) years' experience in a similar position.

Specific Knowledge

- ✓ Understanding and working knowledge of general and financial management principles.
- ✓ Understanding and working knowledge of GOJ's accounting principles, practices, procedures and techniques.
- ✓ Understanding and working knowledge of local financial and economic environment.
- ✓ Understanding and working knowledge of legal and regulatory framework of the SLB.

Skills, Behaviours and Competencies Required

- ✓ Oral and Written Communication
- ✓ Customer and Quality Focus
- ✓ Analytical Thinking
- ✓ Problem Solving and Decision Making
- ✓ Initiative
- ✓ Planning and Organizing
- ✓ Goal/Results Oriented
- ✓ Interpersonal Skills
- ✓ Teamwork and Cooperation
- ✓ Job Knowledge
- ✓ Use of Technology

Remuneration Package

- Basic Salary $6,333,301.00 – $8,517,586.00

Applications along with résumés should be forwarded no later than **Wednesday, January 15, 2025** to:

Manager, Human Resource & Administration Department
Students' Loan Bureau
Sagicor Sigma Building
63-67 Knutsford Boulevard
Kingston 5

E-mail: careers@slbja.com

We thank all applicants for their expressions of interest, however, only shortlisted candidates will be contacted.