GUYANA POLICE FORCE ACADEMY
IT SECURITY POLICY

1. **Preamble**

   1.1. This IT Security Policy outlines the principles, guidelines, and responsibilities for safeguarding Guyana Police Force Academy information assets and IT infrastructure. The policy applies to all academic staff, students, and stakeholders who have access to the Academy's systems and data.

2. **Objective**

   2.1. The Guyana Police Force Academy intention to have a comprehensive IT Security policy that involves addressing various aspects of information and data security within an organization.

3. **Information Security Governance:**

   3.1. The IT Security Officer/Manager job description clearly outlines the roles and responsibilities for information security management.

   3.2. An Information Security Steering Committee is responsible for overseeing security initiatives.

   3.3. Regular risk assessments and audits will identify and mitigate security risks.

4. **Data Protection:**

   4.1. Classifying data based on sensitivity and define appropriate security controls.

   4.2. Ensuring encryption for sensitive data both in transit and at rest.

   4.3. Enforcing data retention and disposal policies to minimize data exposure.

5. **Access Control:**

   5.1. The existence of a least privilege principle for user access to systems and data.

5.2. Use of strong authentication mechanisms, such as multi-factor authentication (MFA).

5.3. Ensuring regular review and update user access rights based on job roles and responsibilities.

6. **Network Security:**

6.1. Ensuring existence of firewalls, intrusion detection/prevention systems, and antivirus software to protect the network.

6.2. Ensuring encrypting network traffic, especially for remote access and sensitive data transmission.

6.3. Ensuring conduct of regular vulnerability scans and penetration testing to identify and remediate network vulnerabilities.

7. **Application Security:**

7.1. Ensuring that software applications are developed and maintained securely throughout their lifecycle.

7.2. Ensuring existence of secure coding practices and conducting regular security assessments of applications.

7.3. Patching and updating software regularly to address known vulnerabilities.

8. **Incident Response:**

8.1. Existence of an incident response team and procedures for reporting and responding to security incidents.

8.2. Documenting incident response plans, including escalation procedures and communication protocols.

8.3. Conduct post-incident reviews to identify lessons learned and improve incident response processes.

9. **Physical Security:**

9.1. Implement physical access controls to secure data centers, server rooms, and other critical infrastructure.

9.2. Monitor and log physical access to sensitive areas.

9.3. Ensure proper disposal of hardware to prevent data breaches.

10. **Employee Awareness and Training:**

10.1. Provides regular security awareness training to all employees.

10.2. Promotes a culture of security consciousness and accountability.

10.3. Conducts phishing simulations and other exercises to test employee readiness.

11. **Compliance and Legal Requirements:**

11.1. Ensure compliance with relevant laws, regulations, and industry standards.

11.2. Regularly review and update security policies to address changing legal and regulatory requirements.

11.3. Maintain documentation and records of compliance efforts.

12. **Enforcement:**

12.1. Defines consequences for non-compliance with security policies and procedures.

12.2. Conducts regular audits and enforcement activities to ensure adherence to security policies.

12.3. Encourages reporting of security concerns and violations without fear of retaliation.

13. **Review and Revision:**

13.1. Regularly review and update the IT security policy to reflect changes in technology, business processes, and threat landscape.

13.2. Solicits feedback from stakeholders to continuously improve the effectiveness of security measures.

14. **EFFECTIVE DATE**

14.1. This policy was approved and has come into effect as of October 25, 2023.

15. **REVIEW PERIOD**

15.1. A review of this policy will be conducted annually. The review will be conducted by the Training Board. The results of the review will be shared with the relevant stakeholders and necessary changes to the policy will be implemented based on the review.

16. **REVISION PERIOD**

16.1. This Policy was revised by the Training Board in January 2024.

17. **APPROVAL OF POLICY**

17.1. This Policy was approved by the Guyana Police Force Executive Leadership Team and the Guyana Police Force Academy Training Board.