GUYANA POLICE FORCE ACADEMY
DATA STORAGE AND MANAGEMENT
POLICY

1. BACKGROUND

1.1. The Guyana Police Force Academy is committed to protecting all staff and students with a safe physical environment as well as an electronic environment. This includes against any data breaching activities, cybercrime, and overall protection of the Academy's data in compliance with the **Access to Information Act 2011** and the **Guyana Data Protection Bill 2023.**

2. OBJECTIVES

2.1. The primary objective of the Data Storage and Management Policy is to establish a comprehensive framework that ensures the secure, efficient, and compliant storage and handling of organizational data.

3. POLICY STATEMENT

3.1. This policy aims to safeguard sensitive information, optimize data accessibility, promote data integrity, and align storage practices with regulatory requirements, thereby mitigating risks and fostering a culture of responsible data management throughout the organization.

4. SCOPE

4.1. Data Ownership

4.1.1. All data stored and managed on the FAPC Server within the institution is the property of the Guyana Police Force Academy.

4.1.2. The Force Training Officer (FTO) is responsible for overseeing data ownership and ensuring compliance with applicable laws and regulations.

4.1.3. Data Classification.

4.1.4. Data shall be classified based on its sensitivity level and potential impact on the organization.

4.1.5. The Data Governance Committee shall be responsible for defining data classification criteria and ensuring consistent application throughout the organization.

4.1.6. Data owners shall be accountable for classifying and labelling data appropriately.

4.2.Data Access

4.2.1. Access to data shall be granted to the commanders of the Academies by the Force Training Officer.

4.2.2. The Force Training Officer is responsible for managing access controls and regularly reviewing and updating user access rights.

4.2.3. The Force Training Officer shall ensure that access to data is granted and revoked promptly, based on changes in job roles or project requirements.

4.3.Data Security

4.3.1. All employees shall be responsible for protecting data from unauthorized access, disclosure, alteration, or destruction.

4.3.2. There shall be the implementation and maintenance of appropriate technical safeguards, including encryption, firewalls, and intrusion detection systems, to protect data from external threats.

4.3.3. Regular security assessments and audits shall be conducted to identify vulnerabilities and implement remediation measures.

4.4.Data Retention

4.4.1. Data shall be retained in accordance with legal, and regulatory requirements.

4.4.2. Data owners shall define retention periods for different types of data and ensure compliance with the defined retention policies.

4.4.3. There shall be the implementation of data backup and disaster recovery procedures to ensure the availability and integrity of data.

4.5.Data Disposal

4.5.1. Data shall be disposed of securely when it is no longer needed or when the retention period has expired.

4.5.2. Data owners shall be responsible for identifying data that can be disposed of and ensuring that appropriate disposal methods, such as secure erasure or physical destruction, are used.

4.5.3. The Force Training Officer shall provide guidelines and tools for secure data disposal and oversee the implementation of these procedures.

5. REPORTING AND COMMUNICATION

5.1.THE FORCE TRAINING OFFICER (FTO) WILL REPORT ALL DATA STORAGE AND MANAGEMENT MATTERS TO:

5.1.1. Commissioner of Police

5.1.2. Deputy Commissioner Operations

5.1.3. Officer-In-Charge Information and Communications Department

5.1.4. Training Board

6. APPROVAL AND EFFECTIVE DATE

6.1. This policy was approved and has come into effect as of October 20, 2023.

7. REVISION DATE

7.1.Revised in February 2024.

8. REVIEW PERIOD

8.1. 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.