GUYANA POLICE FORCE ACADEMY

GPF DATA-CENTER ACCESS AND PHYSICAL SECURITY POLICY

BACKGROUND

The Guyana Police Force Data-Center access and physical security policy is designed to ensure the protection and integrity of sensitive information stored within the data center at the Guyana Police Force Academy. This policy outlines the guidelines and procedures that must be followed by authorized personnel to access the data center and the measures in place to maintain physical security.

To access the data center, authorized personnel must undergo a strict authentication process, including the use of unique identification credentials such as access cards and biometric scanning. These credentials are only issued to individuals with a legitimate need for accessing the data center, such as IT staff or authorized officers.

Physical security measures are in place to prevent unauthorized entry into the data center. These include surveillance cameras, intrusion detection systems, and security guards who monitor the premises 24/7. Access to the data center is strictly controlled, with limited access points and secure entry systems.

Additionally, the data center is equipped with fire suppression systems and environmental controls to ensure the safety and integrity of the stored information. Regular maintenance and testing of these systems are conducted to ensure their effectiveness.

To maintain the security of the data center, strict policies are in place regarding the handling and storage of sensitive information. This includes regular backups, encryption, and secure disposal of data when necessary.

Overall, the Guyana Police Force Data-Center access and physical security policy is designed to protect the confidentiality, integrity, and availability of sensitive information stored within the data center at the Guyana Police Force Academy.

OBJECTIVES

The objectives of having a data-center access and physical security policy within the Guyana Police Force Academy are to:

- ✓ **PROTECT SENSITIVE INFORMATION**: The primary objective is to safeguard the sensitive data stored within the data center. This includes personal information of police officers, confidential investigations, operational plans, and other critical data. By implementing strict access controls and physical security measures, the policy aims to prevent unauthorized access or theft of this information.

- ✓ **ENSURE DATA INTEGRITY**: Another objective is to maintain the integrity of the stored data. The policy outlines procedures for backup, encryption, and secure disposal of data to prevent data corruption, unauthorized modifications, or accidental loss.

- ✓ **MITIGATE RISKS AND THREATS**: The policy aims to identify and address potential risks and threats that the data center may face. This includes physical threats such as theft, vandalism, or natural disasters, as well as cybersecurity threats like hacking and data breaches. By implementing appropriate security measures, the policy helps to mitigate these risks.

- ✓ **COMPLIANCE WITH REGULATIONS**: The policy ensures compliance with relevant laws, regulations, and industry standards regarding the protection of sensitive data. This includes adherence to data protection and privacy laws, as well as any specific requirements for law enforcement agencies.

- ✓ **MAINTAIN OPERATIONAL CONTINUITY**: By implementing measures like regular backups and environmental controls, the policy aims to ensure the availability of

critical data and uninterrupted operations of the data center. This helps to minimize downtime and maintain the functionality of the systems.

POLICY STATEMENT

The Guyana Police Force Academy demonstrates its commitment to the data-center access and physical security policy through the following key commitments:

- ✓ **AWARENESS AND TRAINING**: The academy is committed to ensuring that all personnel, including staff and officers, are educated and aware of the policy. Regular training sessions and awareness programs are conducted to familiarize them with the policy's guidelines, procedures, and their responsibilities in maintaining data security.

- ✓ **STRICT ACCESS CONTROL**: The academy enforces strict access control measures to prevent unauthorized entry into the data center. Only authorized personnel with a legitimate need for access are granted entry, and their access is regularly reviewed and audited to maintain accountability.

- ✓ **PHYSICAL SECURITY MEASURES**: The academy invests in robust physical security measures to safeguard the data center. This includes surveillance cameras, intrusion detection systems, security guards, and secure entry systems. Regular maintenance and testing of these systems are carried out to ensure their effectiveness.

- ✓ **CONTINUAL RISK ASSESSMENT**: The academy is committed to conducting regular risk assessments to identify potential threats and vulnerabilities. This allows them to proactively address any weaknesses in the security infrastructure and implement necessary improvements to mitigate risks.

- ✓ **COMPLIANCE AND AUDITING**: The academy is dedicated to ensuring compliance with relevant laws, regulations, and industry standards related to data security. Regular audits are conducted to assess the effectiveness of security measures and identify areas for improvement.

- ✓ **INCIDENT RESPONSE AND RECOVERY**: The academy has a well-defined incident response plan in place to handle security breaches or incidents promptly and effectively. This includes procedures for reporting, investigating, and resolving security incidents, as well as measures for data recovery and system restoration.

SCOPE

The Communication Officer is responsible for the Data center, everything inside and around, he shall: -

- ✓ Ensure access is controlled to protect both the physical resources and GPF data from unauthorized use, accidental or malicious damage and theft.
- ✓ Define appropriate levels of access (LOAs) allowed based on demonstrated business need.
- ✓ Improve stability and security of systems which store and manage GPF data.
- ✓ Support the GPF's strategy to incorporate information technology as an integral part of decision-making, competitive positioning, and delivery of services.

LEVEL OF ACCESS

Access is controlled to protect both the physical resources and the force's data. Access to the GPF data- center should only be granted when a legitimate need is demonstrated. This access guideline specifies the criteria for granting access to specific individuals or groups, and the different levels of access allowed.

Force Training Officer:

- ✓ Full access to the complete Data Center Access and Physical Security Policy
- ✓ Needs to understand all security protocols, access control procedures, and incident response plans.
- ✓ Must be able to train academy staff and enforce compliance with the policy.

Information Technology Officer:

- ✓ Full access to the complete Data Center Access and Physical Security Policy

- ✓ As the technical lead, requires comprehensive knowledge of data center infrastructure, system configurations, access management, and all security controls.
- ✓ Responsible for implementing and maintaining data center security measures aligned with the policy.

Heads of Departments:

- ✓ Access to relevant sections of the policy pertaining to their department's operations, assets, and personnel.
- ✓ Need to understand security procedures, access restrictions, and requirements specific to their departmental roles and resources within the data center.
- ✓ Accountable for ensuring their staff adhere to applicable portions of the policy.

Academy Instructors:

- ✓ Limited access to the policy focusing on basic security awareness and any procedures specific to their instruction areas.
- ✓ Should be provided training and documentation covering general physical security rules, restrictions, incident reporting, etc. as relevant to their activities.
- ✓ Must follow the security policy themselves and educate students on appropriate conduct.

Students:

- ✓ No direct access to the Data Center Access and Physical Security Policy document
- ✓ Students should receive high-level security awareness education covering the importance of physical security, the need to comply with staff instructions, and any specific student guidelines (e.g. escort requirements, off-limit areas, prohibited actions)
- ✓ Any more detailed procedures would be on a need-to-know basis for students directly involved in data center operations.

The differentiating factor is providing the most comprehensive access and training to those roles with the highest levels of responsibility and authority over data center assets and

operations. IT and training leadership require full policy mastery, while other staff receive tailored guidance aligned with their specific duties and functions related to physical security and access control.

PHYSICAL SECURITY

Entry to the GPF data center will be controlled through physical security, card swipe or keyed entry. Access should only be granted to named individuals and cannot be shared or transferred. The only exception is for emergency personnel, for whom shared access can be granted provided the access credentials (swipe cards/keys) are secured when not in use.

Levels of Access (LOAs)

Full Access, or unsupervised 24×7 access, to the GPF data center, should only be given to individuals with an approved and demonstrated need to access the data center regularly as part of their primary job duties. These individuals can come and go as needed and are not required to log their entries.

Unescorted Access, or “knock then enter” access, to the force’s data center should be given to individuals with an approved and demonstrated need to access the data center on an infrequent basis as part of their job duties. These individuals must gain entry from someone with Full Access and must log their entry and exit to the data center. These individuals do not require an escort while in the data center and must not allow any other person to access the data centre. All Unescorted Access individuals are required to provide identification on demand and leave the facility when requested to do so.

All other individuals are considered unauthorized and granted Escort Only access. These individuals must always be accompanied by an escort, and they must log their entry and exit to the data centre. Any individual with elevated security who fails to present proper identification should be restricted to Escort Only access. All Escort-only access individuals are required to provide identification on demand and leave the facility when requested to do so.

Escorts

Individuals with an LOA of Full Access may escort and supervise unauthorized individuals provided all individuals are logged on entry and exit. An escort must remain in the data center the entire time their guest is in the data center.

Maintenance Staff

Maintenance personnel should be escorted when provided with access to the data center. All maintenance and staff must sign the access log upon entering and leaving the data center. The data center staff must enter any maintenance work in the operations log.

First Responders

First responders, including police, fire and medical are granted unescorted access.

Review

The list of individuals with elevated LOAs, both Full and Unescorted Access, should be reviewed periodically and access should be revoked for any individuals who no longer have a legitimate business need. The data center director should review the list at least every 90 days.

Access Log

A log of access by anyone without an LOA of Full Access must be kept. All such individuals entering a GPF data center must sign the log as they enter and exit the facility for audit and security purposes.

Tours

Tours must be pre-approved by the O/C ITD. All visitors must sign the access log as they enter and exit and must be escorted while touring the data centers.

COMPLIANCE AND ENFORCEMENT

The Guyana Police Force Academies are overseen by the Force Training Officer, Commandant, and Training Inspectors/Supervisors. Instructors are responsible for maintaining the correct instructor-to-student ratio in their classes and exercises. The Police Commissioner and senior administrators are responsible for ensuring the Force adheres to training standards, which may involve allocating resources for staffing and facilities.

REPORTING AND COMMUNICATION

The Academy Commandant is responsible for communicating training regulations, including instructor-to-student ratios, to all personnel and stakeholders. Training Coordinators ensure proper student enrollment and report non-compliance. Instructors inform students about the appropriate ratio for their program and report any concerns. Training Inspectors/Supervisors verify compliance during training sessions and communicate discrepancies. The force Training Officer will communicate policy updates or clarifications regarding training regulations through official channels.

EFFECTIVE DATE

This policy came into effect as of October 26, 2023.

REVIEW PERIOD

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.

REVISION DATE

Revised in January 2024.

APPROVAL OF POLICY

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