

# DATA PRIVACY & INFORMATION PROTECTION POLICY

## 1. Purpose

Ready Guard Security Services (Pvt.) Ltd. ("RGSS") adopts this Data Privacy and Information Protection Policy to ensure that all personal, operational, and organizational data is handled with confidentiality, integrity, and security. The purpose of this Policy is to protect sensitive information, prevent misuse, ensure lawful handling of data, and maintain trust with employees, clients, partners, and stakeholders.

## 2. Scope

This Policy applies to all employees, guards, supervisors, managers, contractors, subcontractors, consultants, vendors, service providers, and any authorized individual with access to RGSS data. It covers personal data, HR records, client information, operational data, digital systems, security-related information, and physical documentation.

## 3. Definitions

**Personal Data:** Information that identifies an individual.

**Sensitive Information:** Data requiring higher protection, including security and operational details.

**Data Processing:** Collecting, storing, using, sharing, modifying, or disposing of information.

**Data Subject:** Any individual whose data is collected by RGSS.

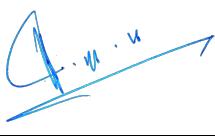
## 4. Policy Principles and Commitments

### 4.1 Lawful and Fair Handling of Data

RGSS collects, processes, and stores data only for legitimate business, legal, or contractual purposes. Data must be collected fairly, used responsibly, and handled in accordance with approved procedures and legal requirements.

### 4.2 Confidentiality and Access Control

Employees must protect all information entrusted to them. Access to data is strictly controlled and granted only on a need-to-know basis. Unauthorized access, sharing, or copying of data is prohibited.

	
Reviewed By	Approved By

#### 4.3 Data Accuracy and Integrity

RGSS ensures data is accurate and up to date. Incorrect or outdated data must be corrected promptly. Manipulation or improper alteration of information is strictly prohibited.

#### 4.4 Secure Storage of Information

Data must be stored securely. Physical files must be locked, and digital data must be stored in secure systems with proper permissions. Passwords must be strong, confidential, and changed when required.

#### 4.5 Data Sharing and Disclosure

Data may only be shared when necessary for business reasons, permitted by law, or approved by management. Data must never be shared with unauthorized individuals.

#### 4.6 Protection during Electronic Communication

Sensitive information must not be sent through insecure communication channels. Company-approved platforms must be used, and files may require password protection or encryption.

#### 4.7 Data Retention and Disposal

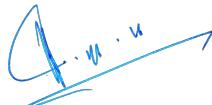
RGSS retains data only for as long as needed. After retention periods expire, documents must be destroyed securely. Digital data must be deleted properly and authorized before removal.

#### 4.8 Reporting Data Breaches

Employees must immediately report lost files, unauthorized access, accidental data sharing, suspicious system activity, or potential breaches. All incidents will be investigated promptly.

#### 4.9 Rights of Data Subjects

Employees and clients may request access to their data, request corrections, or seek clarification on data usage. RGSS will respond within a reasonable timeframe.

	
Reviewed By	Approved By

#### 4.10 Protection of Operational and Security Data

Operational data such as deployment plans, incident reports, and risk assessments must receive heightened protection. This information must never be shared outside authorized channels.

#### 4.11 Third-Party Data Processors

Third parties handling RGSS data must sign confidentiality agreements, use secure systems, and report any breaches immediately. Contracts may be terminated for non-compliance.

### **5. Responsibilities**

Management ensures procedures exist, approves access rights, and monitors compliance. Supervisors ensure proper data handling at worksites. Employees must protect information, avoid misuse, and report concerns immediately.

### **6. Training and Awareness**

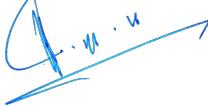
RGSS provides training on confidentiality, secure communication, data protection practices, and breach reporting. Training is refreshed periodically.

### **7. Continuous Improvement**

RGSS reviews privacy practices, legal requirements, and audit findings to strengthen data protection. Policies will be updated as needed.

### **8. Commitment**

RGSS is committed to safeguarding all personal, operational, and organizational information. Data protection supports trust and strengthens organizational integrity.

	
Reviewed By	Approved By