Cyber Security Policy

1. Purpose

Ready Guard Security Services (Pvt.) Ltd. ("RGSS") adopts this Cyber Security Policy to protect digital systems, information assets, networks, and communication channels from cyber threats, unauthorized access, and data breaches. The Policy ensures confidentiality, integrity, and availability of organizational data and supports operational security.

2. Scope

This Policy applies to all employees, guards, supervisors, managers, contractors, consultants, vendors, and any authorized users accessing RGSS systems. It covers all devices, digital platforms, email systems, software applications, cloud services, and communication tools used for RGSS business.

3. Policy Commitments

3.1 Protection of Digital Information and Systems

RGSS ensures that all organizational information, including personal data, operational files, and security-related information, is safeguarded through secure technical and administrative controls. Unauthorized access, duplication, or modification of digital information is prohibited.

3.2 Strong Password and Access Control

Employees must use strong, unique passwords and must not share credentials. Multi-factor authentication must be used where available. Passwords must be changed periodically, and user accounts must be locked when not in use.

3.3 Device Security Requirements

Only authorized devices may be used for RGSS work. Devices must be password-protected, regularly updated, and equipped with approved security software. Lost or stolen devices must be reported immediately.

Reviewed By	Approved By

3.4 Secure Use of Email and Communication Channels

Employees must use company-approved channels for sensitive communication. Confidential data must not be sent through personal email accounts. Suspicious attachments, links, or emails must be reported immediately.

3.5 Internet Use and Online Behavior

Employees must follow safe browsing practices. Downloading unapproved software, accessing unsafe websites, or sharing internal material online is prohibited. Personal use of RGSS systems must remain limited and responsible.

3.6 Data Encryption and Secure Storage

Sensitive digital information must be encrypted during transfer and storage. Files must be stored on secure servers instead of personal devices or unapproved cloud platforms.

3.7 System Monitoring and Logging

RGSS may monitor network activity, access logs, security alerts, and system performance to detect threats and ensure compliance. Monitoring supports risk management and operational safety.

3.8 Protection against Malware and Cyber Threats

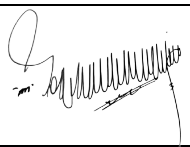
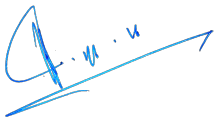
Employees must avoid downloading unverified files and must report suspicious system behavior. Approved antivirus and security tools must remain active and updated.

3.9 Reporting Cyber Security Incidents

Employees must report any suspected cyber incidents such as hacking attempts, phishing messages, system failures, or unauthorized access. Prompt reporting reduces risk and enables immediate mitigation.

3.10 Use of External Storage Devices

USB drives and external storage devices may only be used with approval from management or IT. All devices must be scanned for malware before use.

	
Reviewed By	Approved By

3.11 Protection of Operational and Client Data

All operational and client-related digital information must receive enhanced protection. Deployment plans, incident reports, and security data must never be transferred or shared outside authorized systems.

3.12 Social Engineering Awareness

Employees must remain alert to phishing, impersonation attempts, fraudulent requests, and other social engineering tactics. Sensitive requests must be verified before action.

3.13 Third-Party Cyber Security Compliance

Vendors, contractors, and technology partners must follow RGSS cyber security requirements, use secure systems, and report breaches immediately. Access may be revoked if compliance is not maintained.

4. Roles and Responsibilities

Management must ensure appropriate cyber security controls and resources. IT personnel must maintain system security, monitor threats, and manage access rights. Employees must follow all cyber security rules and report incidents.

5. Training and Awareness

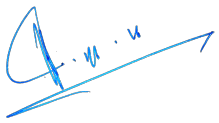
RGSS provides ongoing training on cyber hygiene, password safety, secure communication, and incident reporting. Training strengthens awareness and reduces organizational vulnerability.

6. Continuous Improvement

RGSS evaluates security logs, cyber risks, incidents, and audit findings to update systems and policies. Continuous improvement ensures strong cyber protection.

7. Commitment

RGSS is committed to protecting its digital environment, systems, and information assets. Every employee must follow this Policy and uphold cyber security as a critical responsibility.

	
Reviewed By	Approved By