

RAK Properties PJSC

INFORMATION SECURITY GUIDELINES

DOCUMENT CLASSIFICATION: PUBLIC

Document Owner: Senior Manager – Information Technology

Approved By: CEO, CSSO

1. Purpose

The Information Security Guidelines are extracted from the existing Information Security Policy of RAK Properties. This guideline outlines our commitment to protecting the information assets of RAK Properties from all internal and external threats. It defines principles and responsibilities for ensuring the confidentiality, integrity, and availability of business information and resources, and promotes a security-aware culture across the organization.

2. Scope

These guidelines apply to:

- All employees of RAK Properties, including part-time, contract, and third-party staff
- All information assets owned, controlled, or processed by RAK Properties
- All service providers, vendors, and external partners handling RAK Properties' information

3. Objectives

RAK Properties aims to:

- Ensure the integrity and protection of data across all systems and processes
- Continuously improve the information security management system (ISMS) based on risk assessments, audit findings, and incident learnings

- Monitor and proactively respond to security threats to prevent breaches or reduce their impact
 - Define and enforce individual responsibilities for information security across the workforce
 - Establish clear and enforceable security requirements for third parties, including suppliers, vendors, and contractors
-

4. Core Commitments

4.1 Integrity and Protection of Data

- Information will be classified into Public, Internal Use Only, Confidential, and Secret, with appropriate controls applied to each classification level.
 - All sensitive data must be protected from unauthorized access, alteration, loss, or destruction.
 - Encryption standards will be applied for data in transit and at rest, especially for confidential or secret-level information.
-

4.2 Responsibility for Information Security

- All employees must understand and comply with the Information Security and Acceptable Use Policies.
 - Responsibilities include:
 - Safeguarding passwords and access credentials
 - Following secure handling procedures for information
 - Reporting suspicious activities or incidents
 - Participating in mandatory awareness and training sessions.
 - Disciplinary actions will be taken for non-compliance, as outlined in the HR manual.
-

4.3 Threat Monitoring and Response

- Real-time monitoring systems and intrusion detection tools will be deployed to identify and escalate potential threats.
- An incident management process is in place to:
 - Log and prioritize incidents
 - Initiate containment and recovery actions
 - Investigate root causes

- Review and implement corrective actions.
- Employees must report any observed or suspected security weaknesses immediately.

4.4 Third-Party Information Security Requirements

- All vendors and external service providers must sign Non-Disclosure Agreements (NDAs) and comply with RAK Properties' information security policies.
- Contracts shall define:
 - Scope of access
 - Security expectations (e.g. data protection, access control, incident notification)
 - Audit rights and reporting requirements
 - Termination and data return or destruction procedures
- Remote or physical access by third parties is restricted and subject to prior approval, access logging, and continuous monitoring.

4.5 Continuous Improvement of the ISMS

- The ISMS shall be continuously enhanced through regular reviews, risk assessments, corrective actions, and audits.
- The Information Security Steering Committee (ISSC) will oversee updates and improvements.
- Lessons learned from incidents and new threat intelligence will inform policy revisions and system upgrades.

5. Roles and Responsibilities

Role	Responsibilities
CEO & Executive Team	Approve security policies/guidelines and ensure organizational support
IT Manager / CSSO	Lead ISMS implementation, threat management, and audits
Department Heads	Ensure staff comply with security guidelines within their units
Employees	Adhere to the security guidelines, protect information assets, and report incidents
Vendors & Contractors	Comply with contractual security obligations and RAKP policies

6. Compliance and Enforcement

- Compliance is mandatory and subject to internal audits.
 - Breaches may lead to disciplinary action, contract termination, and/or legal consequences.
 - Policy exceptions must be formally approved by the IT Head and documented.
-

7. Review

These guidelines shall be reviewed at least annually or upon significant changes in regulatory, technological, or operational environments. The review is led by the Information Security Manager and approved by executive leadership.

8. Information Security Management Program

RAK Properties is committed to maintaining a robust and responsive Information Security Management Program (ISMP) to protect its information assets and ensure business continuity. The program is aligned with industry best practices, including ISO 27001 standards, and includes the following key components:

8.1 Information Security Awareness and Training

- All RAK Properties employees must undergo mandatory security awareness training upon onboarding and annually thereafter.
 - Training includes:
 - Phishing awareness and simulated attacks
 - Password hygiene and safe browsing
 - Data classification and handling
 - Mobile and remote work security
 - Periodic campaigns and refresher sessions promote a culture of shared responsibility for information security.
-

8.2 Vulnerability Analysis and Risk Assessment

- Periodic vulnerability assessments and penetration testing are conducted to identify weaknesses in IT systems, applications, and infrastructure.
- Risk assessments consider asset value, threat likelihood, and impact to prioritize remediation efforts.
- Findings are documented in the Risk Register, and mitigation strategies are tracked through to closure.

- Critical vulnerabilities are remediated within defined SLA timelines.
-

8.3 Business Continuity Planning for Information Security

- RAK Properties maintains Information Security, Business Continuity, and Disaster Recovery Plans to ensure continuity of critical operations in the event of system failures, cyber-attacks, natural disasters, or other disruptive incidents.
 - These plans:
 - Define recovery objectives and timeframes (RTO/RPO)
 - Establish backup and restore protocols
 - Identify alternate processing sites and fallback systems
 - The plans are reviewed annually and tested periodically to validate readiness.
-

8.4 Incident Reporting and Escalation

- An incident escalation and response process is in place to enable employees to report security issues quickly and securely.
 - Incidents include:
 - Phishing or suspicious emails
 - Unusual system behaviour
 - Lost/stolen devices or credentials
 - Suspected data breaches or malware infections
 - Reports can be made via:
 - IT Helpdesk
 - Direct escalation to the Information Security Manager or CSSO
 - All incidents are logged, classified, and escalated based on severity. Root cause analysis and mitigation follow the post-incident.
-

8.5 Internal Security Audits

- Internal audits of IT infrastructure and security controls are conducted at least once a year.
- These audits evaluate:
 - Compliance with RAK Properties policies/ guidelines and regulatory requirements
 - Effectiveness of technical and administrative controls

- Configuration baselines and patch management practices
 - Audit findings are reviewed by the Information Security Steering Committee, and corrective actions are tracked to resolution.
-

8.6 Independent External Audit and Certification

- RAK Properties engages independent third-party auditors to perform comprehensive reviews of the ISMS and IT infrastructure.
 - These assessments ensure alignment with international standards such as ISO/IEC 27001.
 - The audit scope includes risk management, access control, encryption, incident handling, asset classification, and third-party management.
 - Certification efforts (e.g., ISO 27001) are supported through documented controls, evidence collection, and gap remediation.
-