cosmicSMS

Cosmic Apps Ltd – 2nd Floor, Nucleus House, 2 Lower Mortlake Road, Richmond. TW9 2JA

The Cosmic SMS Information Security Policy

1. Purpose and Scope

This policy establishes the framework for ensuring the security of information, systems, and personnel in accordance with ISO27001. Its objectives are to:

- Reduce the risk of IT security incidents.
- Ensure business continuity and resilience.
- Safeguard company, client, and employee data.
- Maintain confidentiality, integrity, and availability of information.
- Comply with the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standards (PCI DSS), and other applicable laws and regulations.
- Fulfil professional obligations toward clients and stakeholders.

This policy applies to all employees, contractors, and third-party service providers accessing company systems or handling company data.

---

2. Information Security Objectives

We are committed to:

- Protecting sensitive information against unauthorized access or disclosure.
- Preventing business disruptions caused by IT incidents.
- Maintaining trust with clients, employees, and stakeholders through robust data protection practices.

---

3. Roles and Responsibilities

- **Director of IT Security**: Oversees the IT security strategy and ensures compliance with this policy.
- **IT Operations Manager**: Manages day-to-day implementation of the security policy.
- **Third-Party IT Partner (AWS)**: Provides technical support and assists in implementing security measures.
- **All Employees and Associates**: Adhere to the security guidelines and report security incidents promptly.

---

4. Policy Review and Maintenance

This policy will be reviewed annually. Interim updates may occur to address emerging risks or compliance requirements. Feedback and questions should be directed by email to **info@cosmicsms.com**.

5. Information Classification

We classify information to ensure appropriate protection:

- **Unclassified**: Publicly available information.
- **Employee Confidential**: Includes personal records such as payroll and medical data.
- **Company Confidential**: Covers contracts, source code, passwords, and business plans.
- **Client Confidential**: Includes client personal data, business plans, and sensitive product information.
- **Payment Information**: Governed by PCI DSS for credit card processing.

Confidential information is assumed unless explicitly designated otherwise.

6. Access Control

Access to information is granted on a **need-to-know** basis:

- **Company Confidential**: Role-based access with least privilege; protected by MFA and encryption.
- **Client Confidential**: Access restricted to authorized personnel; data encrypted in transit and at rest.
- **Employee Confidential**: Role-based access with encryption and MFA.

Administrative privileges are limited to authorized personnel: Director of IT Security and the IT Operations Manager.

7. Security Measures

We deploy the following technologies to safeguard our systems:

- **Anti-malware**: Anti-malware is installed on all devices.
- **Email Security**: Spam and malware filtering.
- **Network Security**: Firewalls, auditing and intrusion detection.
- **Data Encryption**: All data is encrypted at-rest.

8. Employee Onboarding and Offboarding

- **Onboarding**: New employees are granted role-appropriate access to systems and receive training on IT security.
- **Offboarding**: Departing employees' access is promptly revoked, and all company data is recovered and confidential information removed from personal devices.

9. User Responsibilities

All employees must:

- Use strong, unique passwords and consider password management tools.
- Report security incidents immediately to the Director of IT Security.
- Ensure that confidential information, whether digital or physical, is protected from unauthorized access.

Device Security:

- Keep software updated and firewalls enabled.
- Use anti-malware tools and avoid installing unnecessary software.
- Enable whole-disk encryption.
- Store files in official company repositories.

General Best Practices:

- Be cautious with email attachments and links.
- Avoid sharing sensitive information unless necessary.
- Exercise vigilance against phishing and social engineering attacks.

10. Physical Security

Confidential information stored on paper must be secured in locked storage when not in use and shredded when no longer required.

11. Incident Reporting and Management

Employees must report all suspected or confirmed security incidents to the Director of IT Security immediately. The company will investigate incidents and take corrective actions to prevent recurrence.

12. Prohibited Activities

The following actions are prohibited:

- Harassment or violation of the company's equality and diversity policies.
- Circumventing security measures or unauthorized access.
- Downloading or installing pirated software.
- Unauthorized disclosure of confidential information.

13. Compliance

This policy ensures compliance with:

- ISO27001: Information Security Management.
- GDPR for data protection.
- PCI DSS for payment data.

Failure to comply with this policy may result in disciplinary action.

Approved By:
Director of IT Security