The Cosmic SMS Information Security Policy

Version 1.2 — Last Revision 07/07/2026. Replaces version 1.1 (26/09/2024).

1. Purpose and scope

This policy establishes the framework for securing information, systems and personnel in accordance with ISO 27001. Its objectives are to:

- Reduce the risk of IT security incidents.
- Ensure business continuity and resilience.
- Safeguard company, client and employee data.
- Maintain the confidentiality, integrity and availability of information.
- Comply with the UK GDPR, the Data Protection Act 2018, PCI DSS and other applicable laws and regulations.
- Fulfil professional obligations towards clients and stakeholders.

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

2. Objectives

- Protect sensitive information against unauthorised access or disclosure.
- Prevent business disruption caused by IT incidents.
- Maintain the trust of clients, employees and stakeholders through robust data-protection practice.

3. Roles and responsibilities

- Director of IT Security — owns the security strategy and ensures compliance with this policy.
- IT Operations Manager — manages day-to-day implementation.
- Third-party infrastructure partner (AWS) — provides technical support for security measures.
- All employees and associates — follow the guidelines and report incidents promptly.

4. Information classification

Information is classified to ensure appropriate protection:

- Unclassified — publicly available information.
- Employee confidential — personal records such as payroll and medical data.
- Company confidential — contracts, source code, passwords and business plans.
- Client confidential — client personal data, business plans and sensitive product information.
- Payment information — governed by PCI DSS.

Information is assumed confidential unless explicitly designated otherwise.

5. Access control

Access is granted on a need-to-know basis, with role-based access and least privilege, protected by multi-factor authentication and encryption. Administrative privileges are limited to authorised personnel: the Director of IT Security and the IT Operations Manager.

6. Security measures

- Anti-malware on all devices.
- Email security: spam and malware filtering.

- Network security: firewalls, auditing and intrusion detection.
- Encryption of data at rest and in transit.

7. Joiners and leavers

New employees receive role-appropriate access and security training. When someone leaves, access is revoked promptly, company data is recovered, and confidential information is removed from personal devices.

8. User responsibilities

- Use strong, unique passwords and consider a password manager.
- Report security incidents immediately to the Director of IT Security.
- Protect confidential information, digital or physical, from unauthorised access.
- Keep software updated, firewalls enabled and whole-disk encryption on; store files in official company repositories.
- Be cautious with email attachments and links, and vigilant against phishing and social engineering.

9. Physical security

Confidential information on paper is kept in locked storage when not in use and shredded when no longer required.

10. Incident reporting and management

All suspected or confirmed security incidents must be reported to the Director of IT Security immediately. Incidents are investigated and corrective actions taken to prevent recurrence.

11. Prohibited activities

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

12. Compliance and review

This policy supports compliance with ISO 27001, the UK GDPR and Data Protection Act 2018, and PCI DSS. Non-compliance may result in disciplinary action. The policy is reviewed annually, with interim updates for emerging risks. Questions: info@cosmicsms.com.