Information security policy

Owner: the Director **Last reviewed:** November 2026

Review cycle: at least annually

Purpose

This policy sets out how Komos Solutions Ltd (“the Company”) protects the confidentiality, integrity and availability of its own information and of information entrusted to it by clients. It is based on practices aligned with ISO 27001 and on the five Cyber Essentials technical controls.

Scope

This policy applies to the Director, to anyone working for the Company, and to associates and partners engaged by the Company. It covers all information, systems, devices and cloud services used for Company business, including client information.

Responsibilities

The Director is responsible for information security, for keeping this policy up to date and for making sure that everyone covered by it understands their obligations. Everyone covered by this policy must follow it and report any actual or suspected security incident immediately.

Principles

- Information is classified according to its sensitivity and handled accordingly.
- Access is granted on a least-privilege, need-to-know basis.
- Risks to information are identified, assessed and treated in proportion to their impact.
- Client information is used only for the purposes agreed with the client.
- Security is considered from the start of every project (security by design).

Technical controls

Firewalls and internet gateways

Devices and networks used for Company business are protected by correctly configured firewalls. Default administrative passwords are changed and unnecessary services are

disabled.

Secure configuration

Devices and services are configured securely, with unnecessary software and accounts removed, and automatic running of untrusted content disabled.

User access control

Each user has an individual account. Administrative privileges are used only when needed and are kept separate from day-to-day accounts. Multi-factor authentication is used for email, cloud services and remote access wherever it is available. Strong, unique passwords are stored in a password manager. Access is removed promptly when it is no longer needed.

Malware protection

Devices are protected by up-to-date anti-malware software, and only software from trusted sources is installed.

Security update management

Operating systems, applications and firmware are kept supported and up to date. High-risk and critical security updates are applied promptly, in line with Cyber Essentials requirements. Unsupported software is removed.

Data protection and encryption

Laptops and mobile devices used for Company business are encrypted and protected by a screen lock. Information is transferred using encrypted channels. Client data is stored only in approved locations and is not copied to personal devices or personal accounts.

Backup and recovery

Important information is backed up regularly, with backups protected from unauthorised access and periodically tested. See the business continuity policy.

Suppliers, associates and partners

Suppliers, associates and partners who handle Company or client information are assessed for their security before being engaged and are bound by written agreements that include confidentiality and security obligations.

Incident management

Security incidents are reported to the Director immediately. The Director assesses the incident, contains it, informs affected clients without undue delay and in line with contractual obligations, notifies the Information Commissioner's Office where required by law, and records lessons learned.

Awareness

Everyone covered by this policy receives security awareness guidance, including how to recognise phishing and social engineering.

Compliance and review

Compliance with this policy is checked periodically. Breaches of this policy may lead to disciplinary action or termination of an engagement. This policy is reviewed at least annually and whenever there is a significant change to the Company's activities or risks.

Komos Solutions Ltd, registered in England and Wales, company number 09084109. Registered office: 3 Westmead Drive, Newbury, Berkshire, RG14 7DJ.