Information Security Policy

Kampakis and Co Ltd (trading as The Tesseract Academy)

Version	Date	Owner	Approved By	Next Review
1.4	December 2024	Fabio Rovai, Operations Lead	Dr Stylianos Kampakis	December 2025

1. Purpose and Scope

This policy establishes the framework for protecting the confidentiality, integrity, and availability of information assets held by Kampakis and Co Ltd (trading as The Tesseract Academy). It applies to all employees, contractors, and third parties who access, process, or manage the organisation's information systems and data.

As an AI consultancy and data science training provider, we handle sensitive client data, proprietary algorithms, research data, and commercially confidential information. This policy ensures that appropriate controls are in place to protect these assets proportionate to the risks identified.

2. Information Security Objectives

- Protect client data and intellectual property from unauthorised access, disclosure, or loss.
- Ensure business continuity and minimise the impact of security incidents.
- Comply with all applicable legal, regulatory, and contractual requirements including UK GDPR, DPA 2018, and the NIS Regulations 2018.
- Foster a culture of security awareness across all staff and associates.
- Continuously improve our security posture through regular review and assessment.

3. Roles and Responsibilities

Role	Responsibility
Managing Director (Dr Stylianos Kampakis)	Overall accountability for information security. Approves policy and resource allocation.
Operations Lead (Fabio Rovai)	Day-to-day management of security controls, incident coordination, policy implementation, and compliance monitoring.
All Staff & Contractors	Comply with this policy and associated procedures. Report security incidents and vulnerabilities promptly.
Third-Party Suppliers	Adhere to contractual security requirements. Notify us of any incidents affecting our data.

4. Access Control

Access to information systems and data is granted on the principle of least privilege. All access is role-based and reviewed quarterly.

- User accounts are created only upon approval from the Operations Lead and are unique to each individual.
- Access rights are reviewed upon role change, project completion, or at least every 90 days.
- Accounts are disabled immediately upon termination of employment or contract.
- Privileged access (administrator accounts) is strictly limited to authorised personnel and subject to enhanced monitoring.
- Multi-factor authentication (MFA) is mandatory for all cloud services, email, and remote access systems.

5. Password and Authentication Policy

Strong authentication is fundamental to our security posture. The following requirements apply:

- Minimum password length of **14 characters** with a combination of uppercase, lowercase, numbers, and special characters.
- Passwords must not be reused across the last **12 password changes**.
- Password managers (e.g., 1Password, Bitwarden) are mandatory for storing credentials. Storing passwords in plain text, spreadsheets, or browser auto-fill is prohibited.
- Multi-factor authentication (MFA) using authenticator apps or hardware keys is required for all business-critical systems.
- Service accounts and API keys are rotated at least every 90 days and stored in secure vaults.

6. Incident Response

All suspected or confirmed security incidents must be reported immediately to the Operations Lead. Our incident response process follows four phases:

6.1 Detection and Reporting

Any individual who identifies a potential security incident must report it within **1 hour** to the Operations Lead via email or phone. Incidents include but are not limited to: unauthorised access, malware infection, data loss, phishing attempts, and physical security breaches.

6.2 Containment

The Operations Lead will assess the incident severity and take immediate containment actions, which may include isolating affected systems, revoking compromised credentials, and preserving evidence.

6.3 Investigation and Resolution

A thorough investigation will be conducted to determine root cause, scope, and impact. External forensic specialists may be engaged for significant incidents. Resolution actions will be documented and tracked.

6.4 Recovery and Lessons Learned

Affected systems will be restored from verified clean backups. A post-incident review will be conducted within 5 working days, and findings will be used to improve controls and update this policy as needed.

7. Acceptable Use

All users of the organisation's information systems must:

- Use systems and data only for authorised business purposes.
- Not install unauthorised software or connect unapproved devices to the network.
- Not share credentials or allow others to use their accounts.
- Lock screens when away from workstations (automatic lock after 5 minutes).
- Not transmit sensitive data via unencrypted channels (e.g., plain email for confidential data).
- Report any suspicious activity or policy violations immediately.

8. Remote Working and Mobile Security

As a remote-first organisation, specific controls are in place for home and mobile working:

- All remote connections to company systems must use an encrypted VPN or zero-trust network access (ZTNA) solution.
- Company data must not be stored on personal devices unless those devices meet our minimum security standards (full-disk encryption, up-to-date OS, endpoint protection).
- Work must be conducted in a private setting where screens cannot be observed by unauthorised persons.
- Portable storage devices (USB drives) are prohibited for transferring company data unless encrypted and pre-approved.

9. Encryption

Encryption is used to protect data at rest and in transit:

- **Data at rest:** AES-256 encryption on all storage devices, databases, and backups.
- **Data in transit:** TLS 1.2 or higher for all web traffic, email (STARTTLS), and API communications.
- **End-to-end encryption:** Used for sharing sensitive client data via approved platforms.
- **Key management:** Encryption keys are stored separately from encrypted data and rotated annually.

10. Physical Security

As a primarily remote-first micro-enterprise, physical security controls focus on:

- Secure home office environments with lockable storage for any physical documents.
- Confidential waste shredding (cross-cut, DIN 66399 Level P-4 minimum).
- Laptop cable locks when working in shared or public spaces.

- No sensitive data stored on local machines beyond encrypted project directories.

11. Backup and Business Continuity

Critical data is backed up to encrypted cloud storage with the following schedule:

- Daily incremental backups of active project data and email.
- Weekly full backups of all systems.
- Monthly backup restoration tests to verify integrity and recoverability.
- Recovery Point Objective (RPO): 24 hours. Recovery Time Objective (RTO): 4 hours for critical systems.

12. Review Schedule

This policy is reviewed annually or following a significant security incident, organisational change, or change in the threat landscape. The next scheduled review is **December 2025**.

Approved by: **Dr Stylianos Kampakis**, Managing Director

Date: December 2024