Holden Knight Group Information Security Policy

1. Purpose

The purpose of this Information Security Policy is to protect Holden Knight Group's information assets from all threats, whether internal or external, deliberate or accidental. Holden Knight Group is committed to maintaining the confidentiality, integrity, and availability of its information, systems, and data to ensure business continuity, minimise risks, and comply with applicable laws and regulations.

This policy applies across all **Holden Knight Group businesses**, including Holden Knight Education and Holden Knight Healthcare, ensuring a consistent approach to security and compliance.

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who access Holden Knight Group's information systems. It covers all business units and client engagements across Holden Knight Education and Holden Knight Healthcare.

Client-specific security requirements may be addressed through separate security addendums, contractual agreements, or additional controls as required.

3. Information Security Objectives

- Protect the confidentiality, integrity, and availability of information.
- Prevent unauthorised access, disclosure, modification, or destruction of information.
- Ensure compliance with legal, regulatory, and contractual obligations.
- Promote a culture of security awareness within the organisation.
- Ensure the proper handling of information security incidents.

4. Responsibilities

Management

Senior management is responsible for establishing and maintaining an effective information security programme. They will ensure that security policies are implemented, resources are allocated, and employees are trained.

Information Security Officer (ISO)

The ISO, currently fulfilled by the Chief Technology Officer, is responsible for overseeing security policies, conducting regular security audits, risk assessments, and ensuring compliance with this policy.

Employees

All employees must adhere to the company's security policies, report security breaches, and complete mandatory security awareness training.

Third-Party IT Security Management

Holden Knight Group engages a third-party IT support provider to manage and oversee IT security, ensuring compliance with this policy and security best practices.

5. Information Security Principles

Confidentiality

Access to sensitive information is restricted to authorised personnel only. Data is classified based on sensitivity and handled in accordance with access control policies.

Integrity

Measures are in place to prevent unauthorised alteration or corruption of data, including encryption, access controls, and regular integrity checks.

Availability

Information and systems are maintained to be accessible when required. This includes reliable backup and recovery systems and protection against threats such as denial of service (DoS) attacks.

6. Security Controls

Access Control

- Access is granted based on the principle of least privilege.
- Strong authentication measures, including multi-factor authentication (MFA), are enforced.
- Regular access reviews are conducted to ensure appropriateness.

Data Encryption

Holden Knight Group primarily utilises Microsoft 365 and Microsoft Azure for cloud services, ensuring security through industry-standard encryption and identity management.

- Data at rest is encrypted using **Azure Storage Service Encryption (SSE)**.
- Data in transit is protected using **TLS 1.2 or higher**.
- Emails and files containing sensitive data are encrypted using **Microsoft 365 Message Encryption (OME)**.

Network Security

- Firewalls and intrusion detection systems (IDS) are in place to protect against unauthorised access.
- Regular security patches and updates are applied to all systems.
- Remote access to company data is restricted to authorised users via Microsoft 365 cloud services, ensuring secure authentication and compliance with access policies.

Endpoint Security

- Company-issued devices have endpoint protection, including antivirus software and encryption.
- Mobile Device Management (MDM) policies are enforced for company devices through Microsoft security policies.
- Bring Your Own Device (BYOD) policies ensure that personal devices used for work meet security standards.

Secure IT Systems and Data Management

Holden Knight Group uses secure, cloud-based IT systems for **finance, recruitment, HR, and operations management**. These systems are protected through access controls, encryption, and compliance with regulatory security standards.

Where software development is part of client engagements, Holden Knight Group ensures secure source code management, vulnerability scanning, and industry best practices in software security.

Data Backup and Recovery

- All critical company data is backed up regularly and securely stored within **UK-based Microsoft data centres**.
- A disaster recovery plan is in place to ensure business continuity.

Security Patch Management

- All company systems and software are maintained with regular security patches and updates.
- Security patches are applied based on risk-based prioritisation to mitigate vulnerabilities.

Incident Management

- All security incidents must be reported to the Information Security Officer.
- An incident response plan is followed to contain, investigate, and mitigate security breaches.
- Lessons learned from incidents are used to improve security measures.

7. Security Awareness and Training

All employees receive mandatory security awareness training covering:

- Phishing and social engineering threats
- Secure password management
- Data handling best practices
- Incident reporting procedures

8. Compliance and Legal Requirements

Holden Knight Group complies with applicable UK and international laws, including:

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990
- Where applicable, industry standards for **healthcare and education security frameworks**, such as the NHS Digital DSP Toolkit.

Holden Knight Group processes all client and employee data within its own IT environment, utilising Microsoft Azure and Microsoft 365 services for secure storage. **No external third-party data processors are engaged unless explicitly stated in a client contract or agreement.**

Holden Knight Group also provides mechanisms for individuals to request access, correction, or deletion of their personal data under **GDPR subject access request (SAR) provisions**.

9. Security Audits and Monitoring

Holden Knight Group will conduct periodic security audits to assess compliance with this policy.

- Security audits will be performed at regular intervals.
- Any identified gaps will be addressed through risk mitigation measures.

10. Data Retention Policy

Holden Knight Group follows a structured **data retention policy** aligned with legal, regulatory, and contractual obligations.

- Personal and business data is **only retained for as long as necessary** to fulfil operational and compliance requirements.
- Secure disposal measures are in place for **data no longer required**, ensuring compliance with the **Data Protection Act 2018** and **GDPR**.

11. Client-Specific Security Requirements

This policy provides a general security framework for all Holden Knight Group clients. Where specific security requirements exist, these will be addressed through **client-specific security addendums, contractual agreements, or additional security controls** as required.

12. Monitoring and Review

This policy will be reviewed annually or in response to significant changes in legislation, business operations, or emerging threats. The Information Security Officer is responsible for ensuring that this policy remains current and effective.

For and on behalf of Holden Knight Group:

Michael Bradley
Chief Technology Officer
March 2025