Information Security Policy

1. Introduction

The Production Hub Limited, ("the Company", "TPH') is committed to safeguarding the confidentiality, integrity, and availability of the information we hold, process, and share. Whether it belongs to our clients, employees, or business partners, information is one of our most valuable assets. Our operations rely on trust — and that trust is built on the assurance that we will manage data responsibly and securely.

This policy sets out our approach to information security and reflects our obligations under UK GDPR, the Data Protection Act 2018, client contracts, and the ISO 27001:2022 standard. We recognise that good information governance underpins business continuity, legal compliance, and the long-term reputation of the company.

This policy applies to everyone working within or on behalf of The Production Hub — including employees, contractors, and third-party service providers. It covers all information assets in our care, whether held in digital systems, cloud platforms like Microsoft 365, or physical records at our premises.

The aim is to ensure that data remains accurate, secure, and accessible when needed — and that everyone understands their role in protecting it.

2. Commitment to Information Security

We are committed to creating an environment in which information is handled with care and protected against threats such as unauthorised access, accidental loss, misuse, or cyber attack. This includes client data, business correspondence, employee records, and commercially sensitive information.

Our approach is built around three core principles: confidentiality, integrity, and availability. We restrict access to information based on job role and business need; we ensure information is accurate and free from unauthorised alteration; and we implement safeguards such as encrypted backups and secure remote access to ensure data is available when required.

Measurable information security objectives are set to support the effective implementation and continual improvement of our Information Security Management System (ISMS). These objectives are aligned with our operational needs, legal and regulatory requirements, and risk-based approach to information management.

3. Legal & Regulatory Obligations

TPH complies with all relevant data protection and information security legislation, including the Data Protection Act 2018 and UK GDPR. We also ensure our practices meet the requirements set out in our client contracts and software licensing agreements.

Where personal data is collected or processed, we do so transparently and lawfully. We have appropriate data processing agreements in place with all clients and suppliers where required. We

continuously review our processes and documentation to ensure we satisfy applicable requirements related to information security and can demonstrate legal compliance.

4. Data Handling & Protection

Information handled by TPH is classified according to its sensitivity, and safeguards are applied accordingly. Personal and commercially sensitive data is encrypted both in transit and at rest. We use secure platforms, including SharePoint and our own SFTP for file transfers, and follow access control protocols that ensure only authorised personnel can view or manage this information.

We retain data for as long as necessary to meet our contractual, legal, and operational obligations. When data is no longer required, it is securely deleted or destroyed in accordance with our internal retention policies.

5. Access & Control Measures

Access to systems and data is granted based on role, with controls enforced through technical safeguards such as password management, MFA, and session monitoring. Access is reviewed periodically, especially during personnel changes or departmental reassignments.

When personnel join or leave TPH, system access and asset control are managed via our HR and IT offboarding processes, ensuring data is protected at every stage of employment.

6. Training, Culture & Responsibility

Information security is a shared responsibility. Every employee at TPH plays a role in maintaining the integrity and protection of our information. To support this, we provide regular training and guidance, starting with induction and continuing through annual refreshers and updates when systems or policies change.

The Information Security Policy and related procedures are available to all staff via our SharePoint system and are referenced in employment contracts and onboarding documents.

We encourage a culture of awareness and openness. Staff are expected to report any actual or suspected breaches of information security immediately to their line manager or the ISMS Manager. All incidents are taken seriously and are managed through our established incident response process, which includes containment, investigation, and lessons learned.

7. Ongoing Monitoring & Improvement

We are committed to the continual improvement of our Information Security Management System (ISMS). This policy is reviewed at least annually or in response to significant operational, legal, or technical changes. Audit results, incident reports, and management reviews form the basis for improvements to our security practices and controls.

Protecting the data we work with is fundamental to our success as a business. TPH is proud of its reputation for reliability and professionalism, and we will continue to invest in the tools, training, and culture required to maintain the highest standards of information security appropriate to the scale and nature of our business.

This policy / policy review has been approved & authorised by:

Name and Position Nick Hames, Director/ISMS Manager

Date: 13/1/26

Signature: 

Policy Review Record	
Effective Date:	January 2024
Last Review:	January 2026
Next Review:	January 2027