INSERT LOGO

STATUTORY, REGULATORY & CONTRACTUAL REQUIREMENTS

Classification: **Public**

This document may be shared with interested parties outside of [Company Name]

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Purpose of This Document

This document identifies and outlines the statutory, regulatory, and contractual requirements applicable to [Company Name].

Compliance with these requirements is integral to our Information Security Management System (ISMS) as per ISO 27001 standards.

Scope

Applicability

The Information Security Policy applies to

- All organisational and customer information, regardless of format.
- All individuals associated with [Company Name], including temporary workers and external contractors.

Monitoring and Review

- The information security manager monitors statutory, regulatory, and contractual requirements changes.
- This table will be reviewed annually and updated as necessary to reflect any legal, regulatory, or contractual obligations changes.

Statutory, Regulatory, and Contractual Requirements

Type	Requirement	Description	Implications	Source
Statutory (UK)	The Data Protection Act 2018	UK law that complements GDPR and addresses specific national issues.	Provides a legal framework for data protection in the UK.	UK Government
	Network and Information Systems Regulations 2018 (NIS)	UK law to improve the cybersecurity of network and information systems across the UK.	Requires essential service operators and digital service providers to implement security measures and report incidents.	UK Government
Statutory (EU)	General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 on data protection and privacy for all individuals within the EU.	Ensures protection of personal data, mandates data breach notification, requires data protection impact assessments, etc.	European Union Law

	ePrivacy Directive (2002/58/EC)	EU directive concerning the privacy and protection of personal data in electronic communications.	Regulates cookies, confidentiality of communications, and traffic data.	European Union Law
Regulatory (UK)	Financial Conduct Authority (FCA) Regulations	Regulations for financial services firms operating in the UK.	Requires firms to manage risks related to information security, data privacy, and operational resilience.	Financial Conduct Authority
Regulatory (EU)	Digital Markets Act (DMA)	Regulation to ensure fair and open digital markets in the EU.	Imposes obligations on gatekeepers to prevent unfair practices.	European Union Law
	Digital Services Act (DSA)	Regulation to create a safer digital space in the EU.	Requires platforms to mitigate risks, ensure transparency, and report illegal content.	European Union Law
Regulatory (US)	Health Insurance Portability and Accountability Act (HIPAA)	US law for protecting sensitive patient data.	Mandates safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI).	US Department of Health and Human Services
	California Consumer Privacy Act (CCPA)	California state law that enhances privacy rights and consumer protection for residents of California.	Grants rights to access, delete, and opt out of the sale of personal data.	State of California
	Federal Trade Commission (FTC) Act	US federal law that prohibits unfair or deceptive business practices.	Enforces data privacy and security standards through regulations and enforcement actions.	US Federal Trade Commission
Contractual	Client Contract A	Contractual obligations with [Client Name] for data protection and information security.	Requires specific security controls, regular security audits, and breach notifications.	Contract with [Client Name]
	Supplier Agreement B	Agreement with [Supplier Name] involving data handling and information security requirements.	Mandates compliance with our information security policies and procedures, regular reporting, and audits.	Contract with [Supplier Name]