[Company]

THIRD PARTY SUPPLIER SECURITY POLICY

Security in third party suppliers

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Third Party Supplier Security Policy

3.1 Purpose

The purpose of this policy is to ensure the data security requirements of third-party suppliers and their sub-contractors and the supply chain.

3.2 Scope

All employees and third-party users.

All third-party suppliers that process, store or transmit confidential or personal data.

3.3 Principle

Third party suppliers meet the requirements of the company, legislation, and regulation for data security.

3.4 Third Party Supplier Register

All third parties are registered and recorded in the Third-Party Supplier Register.

Third parties are assessed for criticality to the business.

Third parties are classified based on the data processed, stored, or transmitted.

In addition, the following is captured as a minimum

- Supplier Name and contact details
- What they do for us
- What data they process store or transmit
- Whether we have a contract and a copy of the contract
- What assurance we have over their data security

3.5 Third Party Supplier Audit and Review

Each third party is subject to audit and review of data security in line with the Third-Party Audit and Review process.

The level of audit and review is based on risk.

3.6 Third Party Supplier Selection

Third parties are selected based on their ability to meet the needs of the business.

Before engaging a third-party supplier, data security due diligence is carried out that includes

- An acceptable level of data security with identified, recorded, and managed risks.
- Appropriate references.
- Appropriate certifications.
- Appropriate supplier agreements and contracts that include data security requirements.
- Legal and regulatory compliance.

3.7 Third Party Supplier Contracts, Agreements and Data Processing Agreements

An appropriate contract, agreement and / or Data Processing Agreement must be in place and enforceable before engaging and third-party supplier to process, store or transmit confidential or personal information.

Third party supplier contracts and agreements include the right to audit.

All company policies apply to the third-party supplier.

The use by third party suppliers of sub-contractors must be approved by a senior manager and the sub-contractor is subject to the same terms and company policies as the third-party supplier.

All third-party suppliers are assessed for their requirements under GDPR and where appropriate privacy impact assessments and data processing agreements are in place.

3.8 Third Party Supplier Security Incident Management

Third party suppliers must have a Security Incident Management process in place.

Third party supplier security incidents that impact confidential or personal information must be reported within 12 hours elapsed of becoming aware of the incident.

Third party supplier security incidents are managed as part of the incident management process.

3.9 Third Party Supplier End of Contract

At the end of the contract the third party will confirm in writing that it has met it contractual and legal obligations for the destruction of company confidential and personal information.

All access to systems and information is revoked.

All assets are returned to the company.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.