SUPPLIER INFORMATION SECURITY POLICY

1. Introduction

Spatial Initiative Ltd provides contracting and professional services to clients in the Commercial, Retail, Banking, Hospitality and Leisure sectors.

Our business relies on IT solutions and applications to share project information which may be accessed by third party suppliers. SIL relies on the integrity and accuracy of project information in order to carry out its business and obligations to our clients. It is therefore essential that information is secured in line with professional best practice as well as statutory, regulatory and contractual requirements that maintain the confidentiality, integrity and availability of all information assets.

SIL has achieved accreditation to the ISO27001:2013 standard and has established an Information Security Management System (ISMS) in accordance with the requirements of ISO27001 and ISO27002 code of practice for information security controls.

The ISMS enables SIL to meet these requirements including those provided by the General Data Protection Regulation (GDPR) and the Information Commissioner's Office (ICO).

2. Purpose

The purpose of this policy is to ensure that all contracts and dealings between SIL and third party suppliers have acceptable levels of information security in place to protect personal data as defined by the GDPR. These requirements are in line with SIL's ISMS, current data protection legislation and information security best practice. This policy sets out SIL's expectations in respect of information security when engaging with third party suppliers.

3. Scope

The scope of this policy applies to any works undertaken on behalf of SIL that involve the sharing of information, either regarding our own businesses or that of our clients including project specific drawings and specifications. The term 'Data' within this policy refers the storing, handling, processing or retention of data including personal data related to SIL, third party suppliers or clients e.g. employee certificates, company health and safety documentation and client project information.

Specific information covered under this policy includes the following:

PROJECT INFORMATION

Project documentation being issued in all formats, must be assessed and only issued if compliant, relevant and necessary to the works being implemented.

Paper copies must be kept to a minimum and consideration given to its disposal through confidential waste arrangements if appropriate.

Should project information in paper media be deemed sensitive it must not be disposed of through normal waste channels. It must be shredded at source, disposed of through our clients confidential waste systems (if approved) or safely returned to premises and disposed of appropriately. Sensitive information can include, but is not limited to:

- Drawings
- Specifications
- Commercial information

OUR CLIENTS FIXED AND LOOSE STORAGE COMPONENTS (E.G. FILING CABINETS, PEDESTALS, CUPBOARDS, SHELVING SYSTEMS)

We will only remove fixed and loose storage components from sites if ALL of the following criteria are met:

- It is labelled and signed by our client or their representative
- Unlocked
- Empty of any loose items or paperwork

SITE SECURITY

SIL will ensure secure and supervised access is maintained to all our clients premises under our control.

Specific areas to be considered include, but are not limited to the following:

- Access for Site Personnel and materials e.g. single access points
- Requirements for manned guarding
- Identification procedures for site personnel and visitors to site
- Secure segregation of site working areas
- Protection of our clients property, equipment and furniture
- Maintaining our clients existing Security and Surveillance Systems at all times.

4. Policy Statement

SIL has robust and well established procurement processes which are designed to ensure solutions and services procured are cost effective, maintain the availability and integrity of information and are fit for purpose. It is therefore important that throughout the procurement and subsequent contractual period SIL is clear on its expectations in terms of information security and supplier responsibilities.

5. Information Security Risks and Requirements for Third Parties

The security of information is the key focus in SIL's ISO27001 risk assessment, procurement and management strategy. Using a risk based and proportionate approach to how information assets should be protected we thereby ensure the security of all data held on our systems in relation to our own business, our clients and our third party suppliers. Having procurement processes which align with identified information asset risks helps to ensure that systems are in place to provide the level and quality of information security required by SIL and the GDPR.

SIL will require each of our third party suppliers to agree to the following in order to be included on our Approved Supplier list:

- Acceptance of our Supplier Information Security Policy
- Confirmation that sufficient anti-virus protection is in place on any machine

6. Supplier Access to SIL Information

SIL will allow third party suppliers to access its information and data where formal contracts and data sharing agreements exist in accordance with the GDPR, SIL's ISMS and where accessing the information is a necessary part of delivering the service requested.

Third party suppliers wishing to gain access to SIL internal systems should request this through the Supply Chain team who will only provide access once the Supplier Information Security Policy has been signed and confirmation has been provided that sufficient anti-virus software is installed on the relevant machines.

Third party suppliers will only be granted access to project information related to works they are undertaking.

Once access is no longer required, the third party supplier will be blocked from our systems.

7. Site Audits

As part of SIL's commitment under the GDPR and its ISO27001 accreditation we **may** seek to undertake an independent Audit of any third party supplier currently working on our behalf if this is deemed necessary to the works being delivered. The Audit review may necessitate a visit to the third party supplier's data centre and/or main office where access to, or processing of, personal data is being undertaken on behalf of SIL. The objective of the site visit(s) will be to assess the adequacy of the physical, logical and operational controls in place and assess whether the supplier's approved IT security procedures are embedded within day to day operations.

8. Security Incident Management

Third party suppliers will be expected to have appropriate security incident management procedures in place. Third party suppliers will be required to notify SIL of any significant security incidents.

Such incidents should be notified as soon as reasonably practical to the SIL's Supply Chain team who will ensure appropriate action is taken.

9. Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to SIL or our clients information, or an event which is in breach of SIL's security procedures and policies. All third party suppliers contracted to provide services, which enable SIL to carry out its business functions and deliver its services to the end client, have a responsibility to adhere to this policy.

All employees and third party suppliers have a responsibility to report security incidents and breaches of this policy as quickly as possible through SIL's Incident Reporting Procedure.

In the case of third party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to SIL internal systems or suspension of contractual arrangements. If damage or compromise of SIL's IT solutions or loss of information results from the non-compliance, SL will remove the third party supplier from the Approved Supplier List and consider potential legal action depending on the severity of the breach.

10. CONFIRMATION OF SUPPLIER COMPLIANCE

We undertake to abide by the provisions contained in the SIL Supplier Information Security Policy and take all reasonable steps to ensure we have in place similar security policies and shall comply with such policies and will be responsible for ensuring that its employees, agents and sub-contractors also comply with such policies.

SUPPLIER ACCEPTANCE

Acceptance by the Supplier Senior Manager (i.e. Managing Director, Chief Executive Officer)

Sign:	Date:
Print:	Title:
Organisation:	
Details of Anti-Virus Software and version:	
Expiry Date of Software:	
Please indicate your typical response time for notifying clients of an information security breach:	