SIG information security & compliance requirements

Information Security

Acceptable Use of and Access to SIG Information Systems

Where the Supplier and/or Service Provider (hereinafter referred to as "Supplier") uses, accesses or interacts with the SIG Network,

(1) Supplier agrees to **process and use the data, programs and resources** of SIG only to the extent necessary to fulfil his contractual obligations. In particular, Supplier is not entitled to access, process or upload changes to any applications, data or programs in any case where this is not essential to the performance of the said contract.

(2) Use and/or **access to the SIG Information Systems** by employees of Supplier shall require prior written notification to SIG, following which SIG will, at its discretion, grant access to such employee(s) by respective credentials (e.g. user ID and password, one-time passwords, public key certificates).

(3) Supplier acknowledges that the use of and the access to the SIG information systems is granted only for the purposes of facilitating the provision of services to SIG under a separate agreement. Therefore, any **private use of e-mail and/or internet** by Supplier and/or its employees or collaborators is strictly forbidden.

(4) Supplier further acknowledges that SIG has put in place technical devices and measures enabling SIG to monitor Supplier's activities within the SIG network, especially with regard to E-mail and Internet use; Supplier hereby explicitly agrees that SIG is entitled to (i) **monitor any activities on SIG Information Systems** of Supplier, Supplier's employees and/or collaborators and (ii) take the necessary measures in the event that such monitoring should reveal that Supplier is in breach of this Agreement.

General Undertaking regarding Internal Control and Information Security

Where the provision of services includes the use of IT-Systems and/or -equipment (whether Supplier or SIG-owned), Supplier undertakes

(1) not to make accessible to any **unauthorized persons** the device used and, where applicable, specified for (remote) access, in particular, not to communicate user ID and password to any third party and to change the password regularly;

(2) to define, document and implement adequate **access control concepts** based on business and security requirements, preventing unauthorized access to (i) SIG information stored on Supplier's information systems and / or storage media or (ii) the SIG information systems through Supplier's own network. Supplier acknowledges that such access control concepts have to (i) clearly state the access control rules and rights for each user or group of users and (ii) include both logical access (such as access to programs and data) and physical access (such as access to buildings or data processing rooms). With respect to the above, Supplier shall have state-of-the-art technology and measures in place or shall accept additional security measures by SIG.

(3) If and to the extent the Supplier is offering services to other companies: to ensure by appropriate **technical, personnel and organizational measures** that the confidentiality of data that is disclosed or accessible to, or processed by, the Supplier in connection with the Services, is not only safeguarded as opposed to third parties, but also as opposed to such other companies (**client separation**).

(4) If and to the extent that the services to be provided by Supplier include the development of or change to software or websites: to define, document and implement **procedures for managing changes to programs and configuration** data according to commonly accepted standards (e.g. ISO 27001, ITIL or COBIT) and to perform all changes according to these procedures. These procedures include that change requests are authorized prior to development, patching, or maintenance activities, that the impact of changes is assessed before authorization and that changes are tested and approved prior to being moved into production.

(5) for **websites**: to conduct state-of-the-art **vulnerability tests** taking into account commonly known vulnerabilities (such as by OWASP) prior to going online and for any major releases;

(6) to do all in its power to ensure that there is no **malicious code** (such as computer viruses) on its computers or systems and that no malicious code is transferred to the SIG information systems. In this respect, Supplier shall have state-of-the-art measures in place (such as anti-virus software) or shall accept additional security measures by SIG;

(7) to **keep strictly confidential** any and all data and information received and/or disclosed to him in connection with the use of SIG information systems and/or the provision of services to SIG and not to disclose such data and/or information to any third party (except, within the scope of fulfillment of obligations, to trustworthy employees bound to secrecy who need to know them in order to perform the contract concluded with SIG), nor to make any commercial use of the data and information without having obtained the prior written consent of SIG. This does not apply to data and information which the Supplier can prove he already had legal right to at the time he received it, or where it was already common knowledge or which would be made legally accessible to Supplier by a third party without any obligation being imposed to keep such data or information secret.

(8) to **irretrievably delete any data** from its computers or other storage media including backup media by using state-of-the-art measures without delay as soon as such data is no longer required for processing purposes and to destroy printouts that are no longer required in such a manner that no misuse is possible;

(9) to **notify SIG** without delay of any (i) **incompliance** (including possible or anticipated) with the requirements set forth herein, (ii) **security incidents** or (iii) any other problems encountered.

Audit & Compliance

The Supplier will perform its obligations under the Agreement, and must procure that its personnel and its subcontractors perform their respective obligations, at all times in compliance with the requirements set out in this Section II.

(1) The Supplier will allow SIG, by appropriate means, to **monitor and evaluate the delivery of the Services** such that any corrective measures that may be required can be taken immediately. The Supplier will grant SIG all access rights (including to systems), and provide SIG with all information, both as necessary for SIG to exercise this monitoring right.

(2) The Supplier grants SIG, SIG's internal auditors and external auditors and their respective designees, the **unrestricted right to audit** the (outsourced) organization and the performance of the Services, in particular the compliance of the Supplier and its subcontractors with this Agreement, applicable laws and policies as well as the accuracy of the charges and invoices.

(3) In order to enable the exercise of the audit right, the Supplier grants SIG, SIG's internal auditors and external auditors and their respective designees, the **unrestricted right to access and/or inspect** (i) all Supplier Locations, including sites of subcontractors, (ii) all relevant documents, media, data and systems related to the Services and to make copies of relevant documents, where necessary for the audit and (iii) all relevant internal processes of the Supplier that are related to the Services, e.g. authorization, identity and access management.

(4) To the extent an audit reasonably requires access to the Supplier's financial records or business secrets or confidential information, the audit may be carried out by a **renowned chartered public accountant** who would report its audit findings only in a summary form to SIG if the Supplier requests this.

Scope and applicability

(1) Where the provisions of Services to SIG requires or results in access to data and/or information relating to **SIG Affiliated Companies**, the obligations of this agreement shall apply accordingly.

(2) Supplier undertakes to **engage any staff member who is required** to use and/or to access the SIG Information Systems accordingly, unless existing agreements with the relevant staff members provide comparable protection.

(3) The Supplier ensures that each of its **subcontractors complies with the above requirements** for information security & compliance with respect to any subcontracted portion of the Services. The contract with the subcontractor must be consistent with this Agreement. The Supplier will ask for SIG's written consent before a subcontractor has initially access to SIG data. Upon request by SIG, the Supplier will provide SIG with a copy of any contract with a subcontractor regarding the Services or parts thereof (excluding pricing information).

Cybersecurity

(1) The Supplier shall comply with the obligations under the Applicable Laws and the Data Protection Laws in relation to all cybersecurity risks associated with the performance of the Contract [and the requirements set out in SIG's Supplier Cyber Security Guidelines.

(2) The Supplier warrants that that its collection, access, use, storage, disposal, and disclosure of Personal Data and Confidential Information relating to SIG, which is used or generated in the performance of this Contract, complies with all Data Protection Laws, other Applicable Laws, and the Contract.

(3) The Supplier shall:

a. secure SIG's and its own data necessary for the performance of the Contract against unauthorized access, modification, destruction, and other misuse,

b. use state-of-the-art technical and organizational measures to ensure data security (e.g., ISO/IEC 27001),

c. provide SIG a contact for all cybersecurity related issues (available during business hours),

d. report to SIG all relevant cybersecurity incidents or Security Breaches occurred or suspected and vulnerabilities discovered in Supplier operations, services, and products, if and to the extent SIG is likely to be affected,

e. fully cooperate with SIG in SIG's handling of any Security Breach, including without limitation assisting with any investigation, and making available all relevant records and data, and

f. use its best efforts to immediately remedy the Security Breach and prevent any further Security Breach.

(4) Upon SIG's request, the Supplier shall provide written evidence of its compliance with this Clause Cybersecurity.

(5) The Supplier shall defend, indemnify, and hold harmless SIG from and against all Damages arising out of or resulting from any third-party claim against SIG arising out of or resulting from Supplier's failure to comply with any of its obligations under this Clause Cybersecurity.

(6) The Supplier acknowledges that any breach of its covenants or obligations under this Clause Cybersecurity may cause SIG irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, SIG may seek equitable relief such as injunctive relief or specific performance, and any other relief that may be available, in addition to any other remedy to which SIG may be entitled under Applicable Laws or in equity. Such remedies are not deemed to be exclusive but are in addition to all other remedies available under Applicable Laws and the Contract, subject to any express exclusion in the Contract to the contrary.

(7) The Parties agree that any breach of this Clause 11 constitutes a material breach for the purposes of Clause Term and Termination.

(8) The Supplier shall, subject to mandatory Applicable Laws, not inform any third party of any Security Breach without the prior written consent of SIG.

Definitions

"**Data Protection Laws**" mean Applicable Laws that concern the processing of Personal Data and data privacy that are relevant to the conduct of each Party under the Contract.

"**Personal Data**" has the meaning given to it under the Data Protection Laws as amended, consolidated, replaced, or updated from time to time.

"**Security Breach**" means an occurrence of a computer malware and spyware, denial of service attacks, denial of service attack extortion, or all known and unknown versions of hacking and extortion.