framatome

Cyber Security – Supplier Undertakings

Definitions:

Supplier	The person named as such in the contract / purchase order, its legal successors in title and permitted assignees.
Customer	The person named as such in the contract / purchase order and its legal successors in title and permitted assignees.
Works	All supplies an services to be furnished or rendered and all works to be performed by the Supplier and its sub-suppliers under a contract with the Customer.
Cybersecurity Incident	Any event resulting from an intentional or unintentional act or omission which damages or may damage an information system or the data that the system processes, stores or transmits, and which requires a response in order to limit its impact.
Feedback	An incident report identifying the vector of compromise of the incident and the proper application of technical and organisational measures to guarantee its remediation.

Clauses:

1. The Supplier declares that it is aware of and agrees to comply with the laws in force relating to computer security, and in particular laws relating to system hacking, remaining in a system without authorisation, deliberate interference with the operation of the system, and fraudulent data manipulation.

2. The Supplier shall notify the Customer upon contract effectiveness of the contact data of its qualified officer in charge of Cyber Security, and inform immediately upon changes thereof during the contract execution phase.

3. In the event the Supplier becomes aware of any unlawful or unauthorized access and/or use of data and/or any IT system of the Customer or the Supplier, or if such an event is suspected by the Supplier, the Supplier undertakes to alert the Customer of such a (suspected) Cybersecurity Incident in writing as soon as it becomes aware of it and/or is notified of it by an authority directly or indirectly controlling it. In such a case, the Supplier shall take all appropriate measures it deems necessary to protect its data and/or IT system and data and/or IT systems of the Customer, including but not limited to suspension of any connection and/or blocking of any access. In no case shall the Customer be held responsible for the consequences of deterioration of the quality of the Works as a result of measures taken in this case.

For any access to the Customer 's IT system, the Supplier shall comply (and shall ensure that its personnel complies) with all the security measures and conditions required to perform the contract, such as the applicable conditions for access to the site and to the Customer 's IT system, which the Supplier has been informed of in writing as well as any security conditions specific to the execution of the contract, as may be referred to in the particular conditions.

The Customer only authorizes the Supplier to access the Customer 's IT system, if agreed in the contract and required for the sole purposes of performance of the contract.
The Supplier shall only use software it has notified to and has been approved by the Customer. The Supplier shall take all necessary precautions to avoid introducing a computer virus into the software, updates and new versions provided to the Customer, and shall take appropriate measures if it notices the existence of such a virus.

4. The Supplier undertakes to take all precautions and measures that the Supplier considers deemed necessary and sufficient so as not to generate, facilitate or induce any Cybersecurity Incident in the scope of Works and/or in the Customer´s information system to which the Supplier has access.

In addition, in the event of any illicit or unauthorised access and/or use of the Customer´s information system referred to in Articles 3 and 4, and/or if such event is suspected, and/or in the event of any other Cybersecurity Incident, the Supplier shall alert the Framatome CERT (Computer Emergency Response Team - Email: it.security@framatome.com - Telephone: (+33) 1 34 96 96 95) as well as the dedicated commercial responsible whose contact details appear in the contract, as soon as they become aware of it and at the latest one (1) calendar day following the (suspected) Cybersecurity Incident.

The Supplier must alert dpit-ge-ciso@framatome.com in Germany in addition to the Framatome CERT.

Any Cybersecurity Incident notified to the Customer shall specify:

- the start date of the incident,
- the scope of Works affected,
- the data affected,
- indicators of compromise (email, exploitation of a network or other vulnerability, propagation vector), and
- any other information that could help the Customer to investigate and remedy the incident.

Until the Cybersecurity Incident is resolved, the Supplier shall:

- Immediately take all appropriate and all necessary measures, including but not limited to:

  (Taking containment measures to limit the scope and consequences of the Cybersecurity Incident;

  (Taking measures to eradicate the threat to information systems by i) deleting malicious code, inappropriate accounts or access, patching of vulnerabilities etc. that are the source of the compromise, and/or ii) updating security solutions or strengthening IT systems and infrastructure in order to prevent the use of tactics, techniques and procedures used in cyber-attacks; and

- keeping the Contractor's CERT informed in writing on a regular basis of the resolution of the Cybersecurity Incident and of any relevant information in respect of the same.

Without prejudice to the foregoing measures to be implemented by the Supplier pursuant to this clause, the Customer may provide support to the extent possible and upon reasonable request from the Supplier, to assist in the resolution of the Cybersecurity Incident.

The Supplier shall prepare and document a Cybersecurity Incident Feedback to track and record information relating to this incident.

The Supplier shall provide the Feedback to the Framatome CERT once the Cybersecurity Incident has been resolved.

In the event of an incident whose introduction or transmission is attributable to the Supplier, the Supplier shall be liable for any damages, losses or any other consequences suffered by the Customer.