Applicable Cybersecurity measures

1. Access to the Buyer's information system

For any access to the Buyer's information system, the Supplier undertakes to comply, both for itself and for its personnel, with all security conditions specific to the performance of the Purchase Order, such as in particular the access conditions in force on the Site concerned and on the Buyer's information system, of which it has been notified in writing and of which it has been made aware prior to any intervention.

The Supplier shall only be authorized by the Buyer to access the Buyer's information system for the purpose of performing the Purchase Order.

If the Purchase Order so provides, the Supplier undertakes not to use any software other than the software of which it has notified the Buyer and which the Buyer has authorized. The Supplier shall take all necessary precautions to avoid introducing a computer virus into the software, updates and new versions supplied to the Buyer, and shall take appropriate measures if it discovers the existence of such a virus.

2. Cybersecurity Incident

The Supplier undertakes to take all precautions and measures that it deems necessary and sufficient in order not to generate, facilitate or induce a Cybersecurity Incident in the context of the services (Goods and/or Services) and/or in the Buyer's information system to which it has access.

In addition, as regards its obligation to alert the CERT Framatome (Computer Emergency Response Team) in the event of a Cybersecurity Incident as soon as it becomes aware of it and no later than one (1) calendar day following the Cybersecurity Incident, the Supplier shall use the following contact details**:**

- Email: it.security@framatome.com
- Phone number: (+33) 1 34 96 96 95.

Any Cybersecurity Incident notified to the Buyer shall specify:

- the contact details of the Supplier's qualified IT contact person,
- the start date of the incident
- the scope of the service affected,
- the data affected,
- the indicators of compromise (email, exploitation of a network or other vulnerability, propagation vector), and
- any other element useful for the remediation and investigation of the incident by the Supplier.

Until the Cybersecurity Incident is resolved, the Supplier shall:

- immediately take all appropriate and all necessary measures without delay, such as, for example and without the following list being exhaustive:
  - taking containment measures in order to limit the scope and consequences of the 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 infrastructures, in order to prevent the use of tactics, techniques and procedures used in cyber-attacks; and
- keep the Buyer'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 .

In particular, the Supplier shall prepare and document a Cybersecurity Incident Feedback to track and record information relating to this incident.

Feedback in the context of these measures means an incident report identifying the vector of compromise of the incident and the proper application of technical and organisational measures to guarantee its remediation. The Supplier shall provide the Feedback to the Framatome CERT once the Cybersecurity Incident has been resolved.