SECURITY
PLASTIVALOIRE GROUP

DATA & CYBER SECURITY MINIMUM REQUIREMENTS IN 'TERMS OF PURCHASE'

As Supplier and a trusted partner of the PLASTIVALOIRE group we rely on you to protect all information relevant to our cooperation with utmost care. This concerns know-how that we share as well as ensuring your ability to deliver products and especially services to us with confidentiality, integrity, availability and constant resilience against cyber-attacks and other threats. If you can have access, collect, store or otherwise process data from or on behalf of PLASTIVALOIRE, Supplier shall at a minimum:

- ⇒ Only access, collect, store or otherwise process Data for the sole purpose of fulfilling Supplier's obligations under the Order, or as otherwise expressly permitted by PLASTIVALOIRE in writing.
- ⇒ Maintain reasonable and appropriate administrative, technical and organizational measures and safeguards to preserve and protect the security, integrity and confidentiality of the Data, aligned with applicable industry standards such as ISO / IEC 27001, TISAX or IEC 62443.
- ⇒ Comply with any other privacy or security policies or procedures that PLASTIVALOIRE may provide or make available from time to time to the Supplier as the context requires.
- ⇒ Use secure tools and procedures to share data with our company to guaranty confidentiality. PLASTIVALOIRE gives tools and procedures for this purpose if needed.
- ⇒ Maintain a reasonable and industry appropriate business continuity plan to ensure its provision of the Supply.
- ⇒ Take into account data and cybersecurity risks included in a comprehensive risk analyses and contingency plan for Solutions in order to assure continuous delivery and operations in the event that supplier detects a confirmed security breach or suspected vulnerability.
- ⇒ In case of a security event impacting PLASTIVALOIRE, Supplier must notify PLASTIVALOIRE within twenty-four (24) hours through the following mail:
    - Mail: it.security@plastivaloire.com
    - Phone: +33 2 47 96 15 15
    - Mail: informatique.support@plastivaloire.com
    - Phone: +33 2 47 96 19 49
  - Such notification shall contain at a minimum:
    - Brief description of the Security Incident,
    - Any PLASTIVALOIRE's data or Data affected by the Security Incident.
    - Any persons involved with the Security Incident, including any persons who made any unauthorized use or received an unauthorized disclosure, if known,
    - What Supplier has done or shall due to investigate the Security Incident, to mitigate any deleterious effects, and to protect against any further harm or other similar Security Incidents; and (e) any other information requested by PLASTIVALOIRE relating to the Security Incident;

The Supplier shall take prompt steps to investigate, contain, and remediate any Security Incident and shall cooperate with PLASTIVALOIRE in any subsequent investigation and response in connection with the Supplier's IT systems or networks, or in relation to the Supply, and shall provide evidence of such activities by providing access to its necessary technical documentation, product risk analyses and detailed list of security measures implemented. Unless otherwise specified hereto, each party will bear its own cost in relation to its performance and action contemplated as determined herein.

In addition to the above and in case the performance of the Order necessitates specific or enhanced protection measures for Data, the Parties will enter into a specific and appropriate addendum considering the level of cybersecurity required by the circumstances as reasonably determined by PLASTIVALOIRE.