AERNNOVA INFORMATION SECURITY REQUIREMENTS FOR SUPPLIERS

SECTION I
SCOPE, DEFINITION AND PERMITTED PURPOSE

1. Scope

1.1 Supplier shall comply in all respects with Purchaser's information security requirements as set forth in this document, and as amended from time to time (the "Infosec Requirements"). The Infosec Requirements apply to (i) Supplier's performance of any Purchase Order or under any Supply Agreement; (ii) all Processing of Confidential Information, and (iii) management of any Information Security Incidents involving Confidential Information.

1.2 These Infosec Requirements do not limit or modify other obligations of Supplier, including under the GTC, any Purchase Order, the Supply Agreement or any Applicable Laws.

1.3 To the extent these Infosec Requirements in any way contradict or conflict with the the GTC or the Supply Agreement, Supplier shall promptly notify Purchaser of the conflict and shall comply with the requirement that is more restrictive and protective of Confidential Information (which may be designated by Purchaser). These commitments apply to Supplier and its Personnel.

2. Definitions

Administrative Safeguards	Means all administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic Information and to manage the conduct of Personnel in relation to the protection of that Information.
Aggregate	Means to combine or store Confidential Information with any Information of Supplier or any third party.
Availability	Means the property that Information is accessible and useable upon demand by an authorized person.
Confidential Information	Shall have the meaning assigned to it in the GTC.
Confidentiality	Shall have the meaning assigned to it in the GTC.
Information Security Incident	Means (i) any actual or suspected compromise, unauthorized access to, use, or disclosure of the Confidentiality, Integrity, or Availability of Confidential Information; (ii) any actual or suspected compromise of, or unauthorized access to, any system that Processes Confidential Information (including Supplier Information System) that presents a risk to the Confidentiality, Availability, or Integrity of Confidential Information; or (iii) receipt of a complaint, report, or other information regarding the potential compromise or exposure of Confidential Information Processed by Supplier.

Integrity	Means the property that Information has not been altered or destroyed in an unauthorized manner.
GTC	Means the General Terms and Conditions of Purchase, as amended from time to time and as available on the Internet at the following URL: https://www.Purchaser.com/en/general-terms-and-conditions-of-purchase-group-Purchaser/.
Physical, Administrative, and Technical Safeguards	Means the controls an organization implements to maintain Information Security, including Physical Safeguards, Administrative Safeguards and Technical Safeguards.
Physical Safeguards	Means physical measures, policies, and procedures to protect electronic Information Systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
Process or Processing	Means any operation or set of operations on data, such as access, use, collection, receipt, storage, alteration, transmission, dissemination or otherwise making available, erasure, or destruction.
Technical Safeguards	Means the technology, and the policies and procedures for its use, that protect electronic Information and control access to it.

Further to that, all other definitions or capitalized terms not included in this clause shall have the meaning assigned to them in the GTC or in the Supply Agreement.

3. Permitted Purposes

3.1 Supplier shall Process Confidential Information only to the extent expressly authorized under the Agreement, and only for the purposes expressly authorized under such Agreement (hereinafter, "Permitted Purpose").

3.2 Supplier shall not transfer, rent, barter, trade, sell, rent, loan, lease, or otherwise distribute or make any Confidential Information available to any third party.

3.3 Supplier shall not Aggregate Confidential Information, even if anonymized or pseudonymized, except as expressly authorized under the Agreement.

SECTION II
INFOSEC REQUIREMENTS

Unless otherwise provided for elsewhere, the terms and conditions in Section 2 are only applicable if Supplier receives Confidential Information and Processes it on Supplier's network or Supplier Information System.

4. Information Security Requirements

4.1 General security requirement. Supplier shall maintain Physical, Administrative, and Technical Safeguards consistent with industry-accepted best practices (including the International Organization for Standardization's standards ISO 27001 and 27002, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or other similar industry standards for information security) to protect the Confidentiality, Integrity, and Availability of Confidential Information.

4.2 Specific safeguard requirements. In addition to following the above standards, Supplier's Information security program shall include, at a minimum, the following safeguards and controls:

(a) Written information security program. Supplier shall implement a written information security program, including appropriate policies, procedures, and risk assessments, which shall be reviewed at least annually. The program shall apply to Supplier's Personnel and subcontractors.

(b) Security awareness training. Supplier shall provide periodic training to its Personnel on security, relevant threats and business requirements (such as, v.gr., social-engineering attacks, sensitive data handling, causes of unintentional data exposure, and Information Security Incident identification and reporting).

(c) Data inventory. Supplier shall document and maintain information regarding how and where Confidential Information is Processed while under Supplier's possession or control.

(d) Secure configurations. Supplier shall manage security configurations of its Information Systems using industry best practices to protect Confidential Information from exploitation through vulnerable services and settings.

(e) Controlled use of administrative privileges. Supplier shall limit and control the use of administrative privileges on computers, networks, and applications consistent with industry best practices.

(f) Vulnerability and patch management. Supplier shall maintain a process to timely identify and remediate system, device, and application vulnerabilities through patches, updates, bug fixes, or other modifications to maintain the security of Confidential Information.

(g) Maintenance, monitoring, and analysis of audit logs. Supplier shall collect, manage, retain, and analyze audit logs of events to help detect, investigate, and recover from unauthorized activity that may affect Confidential Information. Logs shall be kept and maintained for at least six (6) months.

(h) Malware defenses. Supplier shall deploy anti-malware software to control and detect the installation, spread, and execution of malicious code; and shall configure all workstations and servers on Supplier's network to that effect.

(i) Firewalls. Supplier shall implement and maintain firewalls to protect systems containing Confidential Information from unauthorized access. Supplier shall review firewall rule sets at least annually to ensure valid, documented business cases exist for all rules.

(j) Suitable Environment. Information shall be used in an environment suitable to its purpose. V.gr., production data shall not be used on test equipment and test data shall not be used on production equipment.

(k) Change Management. All changes to production systems shall be tracked, recorded, and reviewed.

(l) Disablement of services. Supplier shall disable all unnecessary services, protocols, and ports. Authorized services shall be documented with a business justification and be expressly approved.

(m) Encryption. Supplier shall encrypt all Confidential Information at rest and when in transit across open networks in accordance with industry best practices. Upon Purchaser's written request, Supplier shall confirm that all copies of encryption key have been securely deleted.

(n) Access controls. Supplier shall implement the following access controls with respect to Confidential Information:

- Unique IDs. Supplier shall assign individual, unique IDs to all Personnel with access to Confidential Information, including accounts with administrative access. Accounts with access to Confidential Information shall not be shared.
- Need-to-know. Supplier shall restrict access to Confidential Information to only those Personnel with a "need-to-know" for a Permitted Purpose.
- User access review. Supplier shall periodically review Personnel and services with access to Confidential Information and remove accounts that no longer require access.

(o) Account and password management. Supplier shall implement account and password management policies to protect Confidential Information, including, but not limited to:

- No default passwords. Before deploying any new hardware, software, or other asset, Supplier shall change all default and manufacturer-supplied passwords to a password consistent with the password strength requirements described below.
- Inventory of administrative accounts. Supplier shall maintain an inventory of all administrative accounts with access to Confidential Information and shall provide a list of these accounts to Purchaser at Purchaser's request.
- Password strength. Supplier shall ensure that all Personnel use strong passwords by enforcing the following minimum requirements:
    - passwords shall be of a minimum length of 8 characters;
    - passwords shall not match commonly used, expected, or compromised passwords; and
    - Supplier shall force a password change if there is evidence the password may have been compromised.
- Credential encryption. Encrypted passwords and other secrets shall be stored in an industry-accepted form that is resistant to offline attacks (such as password management tools).

(p) Data segregation. Except where expressly authorized by Purchaser in writing, Supplier shall logically and physically isolate Confidential Information at all times from Supplier's and any third-party information.

(q) Personnel security and nondisclosure. Purchaser may condition access to Confidential Information by Supplier Personnel on Supplier Personnel's execution and delivery to Purchaser of individual nondisclosure agreements, the form of which shall be specific by Purchaser. If requested by Purchaser, Supplier shall obtain and deliver to Purchaser signed individual nondisclosure agreements from Supplier Personnel that shall have access to Confidential Information before granting access to Personnel.

4.3 Access to Purchaser Extranet and Supplier portals. Purchaser may grant Supplier Personnel access to Confidential Information via web portals or other non-public websites or extranet services on Purchaser's or a third party's website or system (each, an "Extranet") for the Permitted Purposes. If Purchaser permits Supplier to access any Confidential Information using an Extranet, Supplier shall comply with the following requirements:

(a) Permitted Purpose. Supplier and its personnel shall access the Extranet and access, collect, use, view, retrieve, download or store Confidential Information from the Extranet solely for the Permitted Purpose.

(b) Accounts. Supplier shall ensure that Supplier Personnel use only the Extranet account(s) designated for each individual by Purchaser; shall require Supplier Personnel to keep their access credentials confidential; and shall ensure that accounts are not to be shared.

(c) Systems. Supplier shall access the Extranet only through computing or processing systems or applications running operating systems managed by Supplier and that include: (i) system network firewalls in accordance with clause 4.2(i) (i)(firewalls); (ii) centralized patch management in compliance with clause 4.2(f) (vulnerability and patch management); (iii) appropriate anti-malware software in accordance with clause 4.2.(h) (malware defenses); and (iv) for portable devices, full disk encryption.

(d) Restrictions. Except if previously authorized in writing by Purchaser, Supplier shall not download, mirror or permanently store any Confidential Information from any Extranet on any medium, including any machines, devices or servers.

(e) Account Termination. Supplier shall terminate the account of each of Supplier's personnel and notify Purchaser no later than 48 hours after any specific Supplier personnel who has been authorized to access any Extranet (a) no longer needs access to Confidential Information or (b) no longer qualifies as Supplier personnel (e.g., the personnel leaves Supplier's employment).

5. Security Reviews and Audits

5.1 Upon Purchaser's request, Supplier shall complete risk assessment questionnaires, and confirm in writing to Purchaser Supplier's compliance with these Infosec Requirements.

5.2 In addition to the above, and upon Purchaser's written request, and in order to confirm Supplier's compliance with these Infosec Requirements, Supplier grants Purchaser (or, at Purchaser's election, a third party on Purchaser's behalf), permission to perform an assessment, audit, examination, or

review of the Physical, Administrative and Technical Safeguards in place to protect Confidential Information Processed by Supplier. Supplier shall fully cooperate with the assessment.

5.3 Remediation. Supplier shall promptly address any exceptions or deficiencies identified during Purchaser's security review or in any audit report, by developing and implementing, at Supplier's sole expense, a corrective action plan agreed to by Supplier and Purchaser.

6. Information Security Incidents

6.1 Supplier shall have documented processes and incident response plans that address Information Security Incidents (which shall be a set of written instructions and Countermeasures including but not limited to detecting, responding to, and limiting the effects of an Information Security Incident), and provide to Purchaser a copy of those processes and plans upon request.

6.2 Supplier shall notify Purchaser (within 72 hours of discovery), of any Information Security Incident, and (at Supplier's expense, and without prejudice to any other applicable safeguarding requirements, remedies, or obligations regarding the protection of Confidential Information) shall:

- immediately investigate any Information Security Incident;
- make all reasonable efforts to secure Confidential Information and mitigate the impact of the Information Security Incident;
- remedy each Information Security Incident in a timely manner following its response plan and industry best practices;
- provide timely and relevant information to Purchaser about the Information Security Incident on an ongoing basis; and
- cooperate with Purchaser in the manner defined in this section.

6.3 Supplier shall reasonably cooperate with Purchaser in Purchaser's handling of an Information Security Incident, including, without limitation: (i) coordinating with Purchaser Supplier's response plan; (ii) assisting with Purchaser's investigation of the Information Security Incident; (iii) facilitating interviews with Supplier's Personnel and others involved in the Information Security Incident or response; and (iv) making available all relevant records, logs, files, data reporting, forensic reports, investigation reports, and other materials, required for Purchaser to comply with Applicable Laws, regulations, or industry standards, or as otherwise required by Purchaser.

6.4 Supplier shall respond promptly and appropriately to any inquiries from Purchaser related to compliance with this section (including documentation and/or independent evidence of the effectiveness of implemented controls, processes and Countermeasures mentioned above).

6.5 Supplier shall provide prior written notification of any material changes to Supplier Information System, in particular where those changes include any new third party that shall store, Process, or transmit Confidential Information on Supplier's behalf.

[LEFT INTENTIONALLY BLANK. SEE NEXT PAGE FOR SIGNATURES.]

By means of this document and signature, the duly appointed representative of Supplier declares that it has read and understood, and accepts and agrees to comply with, any and all of Aernnova's Infosec Requirements.

Complete name of Supplier _____

Supplier's representative full name _____

Date _____

Signature _____