Welcome to Mölnlycke's Supplier Information Security Requirements Portal

As a valued business partner to Mölnlycke, it is essential that the products and/or services you provide meet our standards for information security. The following information security requirements (the "**ISR**") outline the necessary measures and expectations to ensure the protection of data and systems throughout our collaboration and apply to all products and/or services provided to Mölnlycke by you, in your capacity as a supplier and business partner. These requirements form an integral part of, and shall be read in conjunction with, the applicable agreement between you and Mölnlycke (the "**Agreement**"). By providing products and/or services to Mölnlycke, you acknowledge and agree to comply with these requirements, which are designed to safeguard the confidentiality, integrity, and availability of information and systems relevant to Mölnlycke's operations.

1 DEFINITIONS

1.1 All capitalised terms and expressions used in the ISR that are not specifically defined herein shall have the same meaning as ascribed to them in the NIS2 Directive. In the absence of such a definition in the NIS2 Directive, the definitions set forth in the Agreement shall apply.

1.2 "Backup" refers to the process of copying and archiving data to ensure it is available for recovery in the event of data loss or disaster.

1.3 "Customer Data" refers to all data, material and information processed by the Supplier in course of performing the Services which originate from Mölnlycke or the Service Recipients or from third-parties in whatever form that data and/or information may exist.

1.4 "Information Security" refers to the protection and preservation of Confidential Information, data, applications, systems, and network resources from accidental or deliberate misuse through unauthorized disclosure, alteration, or destruction.

1.5 "Login Credentials" means a unique username and password.

1.6 "Multifactor Authentication" is a security process that requires two or more distinct forms of identification for user access. This includes a combination of something the user knows (password), something the user has (smart card/token), and something the user is (biometrics).

1.7 "NIS2 Directive" refers to the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), including any relevant national legislation implementing or supplementing the NIS2 Directive in the Member States.

1.8 "Security Incident" means any event or series of events that compromises or poses a threat to the availability, authenticity, integrity, or confidentiality of data, systems, or network and information services. For example:

- unauthorized access, use, disclosure, alteration, or destruction of data, systems, or network infrastructure;
- unplanned service disruptions or denial-of-service attacks;
- unauthorized processing, storage, or transmission of data;
- any unauthorized modification of system hardware, firmware, or software;
- any event that, based on its technical characteristics, may have the potential to cause significant material or non-material damage to an entity or its users.

1.9 "Service Recipients" means all Mölnlycke's Affiliates unless expressly otherwise agreed.

2 INFORMATION SECURITY OBLIGATIONS

Security Requirements

2.1 The Supplier shall ensure that basic and appropriate security protection measures are implemented and maintained for any service provided under the Agreement. These measures should include, but are not limited to:

(a) Information Security;

(b) Physical security;

(c) Access controls;

(d) Incident response.

The Supplier is encouraged to align with recognized security frameworks such as ISO/IEC 27001 or equivalent. If not certified, the Supplier should be able to demonstrate general awareness and application of good security practices. Where relevant, the Supplier should:

i. Ensure security systems and tools are used only for their intended purpose;

ii. Promote basic security awareness among personnel, including onboarding training and periodic updates;

iii. Ensure that key personnel handling information or systems have appropriate competence or experience;

iv. Avoid altering any security measures specified by Mölnlycke without prior agreement.

Physical Security

2.2 The Supplier shall ensure that all premises used for activities related to Mölnlycke are equipped with reasonable and proportionate physical and environmental protection measures. At a minimum, this includes intrusion protection, fire alarms, and access control systems. Where applicable, servers and communication equipment handling Mölnlycke-related services shall be located in areas that restrict access to authorized personnel only. The Supplier is encouraged to maintain basic routines to protect systems and services against damage or disruption caused by fire, water, power outages, or similar foreseeable risks.

Organization of Information Security

2.3 The Supplier shall maintain basic security policies and procedures appropriate to the nature of the services provided to Mölnlycke. These policies should support the identification and management of key security risks. The Supplier shall ensure that staff changes affecting personnel with access to Mölnlycke's systems are appropriately documented and made available for review upon request. Where legally permissible, the Supplier shall conduct reasonable screening of personnel who have access to Mölnlycke's information.

Encryption Requirements

The supplier shall establish, implement, maintain, and apply policies and procedures related to cryptography, with the purpose of ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of Mölnlycke's data (both at rest and in transit).

2.4 The Supplier shall carry out the following encryption measures:

i. Removable media and mobile computer equipment containing Confidential Information shall be password protected and encrypted.

ii. Establish the protocols or families of protocols to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices to be approved and required for use in Mölnlycke, following, where appropriate, a cryptographic agility approach.

iii. Establish safe methods for logging and auditing of key management-related activities.

iv. Utilize dedicated encryption keys. All encryption keys used to protect Confidential Information under the Agreement shall be uniquely associated to Mölnlycke. The use of said encryption keys to encrypt non-Mölnlycke Customer Data is forbidden.

v. Establish methods for dealing with compromised keys and revoking keys including how to withdraw or deactivate keys.

vi. Establish methods for recovering lost or corrupted keys, backing up or archiving keys and destroying keys.

vii. All encryption keys will be protected against modification. Secret and private keys need to be protected against unauthorized disclosure. The Supplier shall establish safe and secure methods for storing keys, including how authorized users obtain access to keys, changing or updating keys, including rules on when and how to change keys.

viii. Establish methods for setting activation and deactivation dates for keys ensuring that the keys can only be used for the specified period of time according to Mölnlycke's rules on key management.

ix. Whenever cryptographic services are applied, only FIPS-approved or NIST-recommended cryptographic algorithms commensurate with key size shall be used.

x. Implement full-disk encryption on any built-in or removable storage media in any Supplier-controlled portable computer which may access, store, transmit, or process Confidential Information under the

Agreement. All such encryption shall minimally meet the Advanced Encryption Standard with a 256-bit cypher key ("AES256").

xi. Ensure that all passwords are transmitted securely and encrypted when in storage. In the event that a hashing algorithm is used, Supplier must use a randomly generated salt.

xii. Plaintext encryption and/or decryption keys must be adequately secured. Only trusted personnel from the Supplier who have a "need to know" should be given access to the key or security environment storing keys. Storage of these keys must be separate and distinct from the encrypted data.

xiii. When a cryptographic key is compromised, all use of the key to apply cryptographic protection to information (e.g., compute a digital signature or encrypt information) shall cease, and the compromised key shall be revoked. However, the continued use of the key under controlled circumstances to remove or verify the protections (e.g., decrypt or verify a digital signature) may be warranted. All compromised keys must be retired and replaced in a timely fashion. The Supplier should have a compromise-recovery plan for restoring cryptographic security services in the event of a key compromise.

xiv. The Supplier's encryption key management systems should be designed so that the compromise of a single key compromises as little data as possible and avoids having a catastrophic weakness.

xv. Encryption keys will not persist unencrypted in any environment, beyond the minimum time required for use. To the maximum extent operationally possible, plaintext symmetric and private keys are restricted to physically protected containers. This includes key generators, key-transport devices, key loaders, cryptographic modules, and key-storage devices.

xvi. Ensure that all Confidential Information stored in any cloud based solution is encrypted per all the aforementioned encryption requirements.

Infrastructure Security

2.5 The Supplier shall apply the following Infrastructure Security controls:

i. The Supplier must ensure the recoverability of Customer Data with off-site backups stored separately from the primary data location. Confidential Information and Customer Data on physical media must be securely destroyed or returned after termination of the Agreement. Documented destruction routines shall be maintained, and proof of destruction provided upon request. Access to backups shall be controlled.

ii. The Supplier shall monitor its services for deviations from access policies and potential Security Incidents. Security logs must be reviewed on a regular basis, and Security Incidents reported to Mölnlycke without undue delay. The Supplier shall present its log review routine upon request.

iii. The Supplier shall ensure that adequate and up-to-date malware protection is implemented at all times. Therefore, the Supplier shall install, enable and keep current reputable, commercially available anti-malware software on all servers and mobile computer equipment used in accessing, processing, transmitting, or storing Confidential Information.

iv. The Supplier shall apply critical and high-risk patches in a timely manner and conduct vulnerability scans on externally-facing systems. Identified vulnerabilities shall be addressed appropriately.

v. Communication channels must be appropriately secured. Confidential Information must be encrypted during transmission. Wireless networks shall use WPA2 or equivalent encryption.

vi. The Supplier shall follow documented routines for remote access and ensure industry-standard protection for external connections. Remote sessions involving Confidential Information must be performed via a secure Virtual Private Network (VPN). The Supplier is responsible for protecting Confidential Information, including secure disposal or overwriting of media and encryption of mobile devices.

vii. Only authorized Supplier personnel may access Mölnlycke's systems and services. The Supplier shall maintain a process to manage user access and provide a list of authorized personnel upon request. All personnel with access to Confidential Information must use unique Login Credentials.

viii. A password shall expire no less often than every ninety (90) days. Said password shall be at minimum 8 characters in length, include at least three of the following: alpha, numeric, special character, and case sensitivity. Additionally, said password shall not contain any portion of username, shall change every ninety (90) days maximum, and not be reused for a minimum of 365 days. The Supplier shall ensure that Login Credentials are terminated in a timely manner upon the removal of its personnel from provision of the Service(s) for any reason. Multifactor Authentication must be implemented where possible.

Human Resources Security

2.6 The Supplier must ensure a thorough understanding and commitment to Mölnlycke's security responsibilities, relevant to the services provided and the specific job requirements, in accordance with Mölnlycke's at any time applicable policy on the security of network and information systems. The Supplier is also required to comprehend and adhere to the standard cyber hygiene practices implemented by Mölnlycke.

2.7 **Security in Software Development and Maintenance**
The Supplier shall follow secure and documented software development practices. Vulnerability testing must be performed regularly, with significant findings resolved in a timely manner. For systems exposed to the internet, such testing shall be conducted at least annually. Test results shall be shared with Mölnlycke upon request or in case of any critical findings.

Regulatory Compliance

2.8 The Supplier must, where applicable, be certified according to the ISO management system standard (e.g., ISO 9001; ISO 27001; ISO 14001), and/or to a sector-specific management system standard (e.g., ISO 13485). Furthermore, the Supplier must comply with the software validation requirements and maintain design and change control processes including software validation in accordance with the latest Good Automated Manufacturing Practice. Validation efforts must ensure that all systems affecting regulated data are fit for purpose, meet documented user requirements, and are maintained in a validated state. Validation records must be maintained and provided to Mölnlycke upon request.

2.9 The Supplier shall maintain the qualified state of relevant IT infrastructure through appropriate incident, change, and service level management practices. ISO 9001 and ISO 27001 certifications are strongly recommended. If available, the Supplier should share relevant third-party audit reports (e.g., ISAE 3402 Type 1 or 2) with Mölnlycke upon request.

2.10 Personnel must have relevant education, training, or experience for working with GxP-supporting software, where applicable. Training records shall be maintained and made available to Mölnlycke upon request.

Incident Reporting

2.11 The Supplier shall follow Mölnlycke's policies and mechanisms to report suspicious events to Mölnlycke.

2.12 The Supplier shall establish formal incident response policies and procedures according to recognized industry standards, which shall include at least the following stages;

(a) incident containment, to prevent the consequences of the incident from spreading;

(b) eradication, to prevent the incident from continuing or reappearing; and

(c) recovery from the incident, where necessary.

2.13 The Supplier shall fully cooperate with Mölnlycke in any incident investigation and take necessary actions to comply with all applicable Laws and Data Protection Laws. In the event that an incident results from the Supplier's failure to meet the security obligations outlined in the Agreement, Mölnlycke reserves the right to impose penalties, including but not limited to termination of the Agreement and/or financial damages for losses incurred. In the event of a Security Incident(s), the Supplier shall collect, retain, and present evidence in support of potential legal action in accordance with the rules for evidence in the relevant jurisdiction. The Supplier shall, if requested, provide applicable information, including but not limited to, forensic copies, network and activity logs, and reasonable access to assist Mölnlycke in investigating.

2.14 Supplier shall, as soon as Supplier is aware of any Security Incident(s) occurring and within 12 hours, provide all necessary information to Mölnlycke so that Mölnlycke can (if necessary) report an early warning to the competent authorities within 24 hours from the time the Security Incident was discovered. Such information shall include whether the incident is suspected of being caused by unlawful or malicious acts or could have cross-border implications.

2.15 Supplier shall, after providing the information for an early warning as per above, provide Mölnlycke with the information necessary for Mölnlycke to make an incident notification to the competent authorities within 72 hours, updating the early warning information and providing an initial assessment of the Security Incidents(s) severity, impact, and indicators of compromise, if available.

2.16 Upon request, the Supplier shall submit an intermediate report to Mölnlycke detailing relevant status updates regarding the Security Incident.

2.17 Supplier shall provide Mölnlycke with all necessary information for Mölnlycke to submit a final report to the competent authorities no later than one month after the incident notification, including a detailed description of the Security Incident, its severity and impact, the type of threat or root cause, applied and ongoing mitigation measures, and any cross-border implications, if applicable. If the Security Incident is ongoing at

such time, the Supplier shall provide the information necessary for Mölnlycke to provide a progress report to the competent authorities.

Business Continuity and Disaster Recovery

2.18 The Supplier shall maintain a business continuity and disaster recovery plan to address potential disruptions of Service(s). The plan shall include procedures for restoring services and maintaining operations in the event of a disruption. The Supplier shall review this plan periodically to ensure it remains relevant and shall provide a copy to Mölnlycke upon request. In the event of a disruption, the Supplier shall notify Mölnlycke promptly and in any event within twenty-four (24) hours, and provide an overview of the recovery efforts.

Mobile Device Security

2.19 The Supplier shall ensure that appropriate measures for securing portable devices are explained to and followed by all personnel. This includes, but is not limited to, any time the device is not in a secured office location (e.g., automobiles, aircraft, home, etc.). The Supplier shall create and maintain policies and standard which provide guidance on transporting and securing devices which may contain Confidential Information when outside of a secured office location.

Compliance with the NIS2 Directive and Derived Laws

2.20 The Supplier and its sub-suppliers, where applicable, shall comply with all relevant requirements of the NIS2 Directive and any local legislation derived from it in the respective Member States. This includes, but is not limited to:

a) Conducting regular cyber risk analyses;

b) Implementing incident response protocols;

c) Maintaining and updating business continuity and disaster recovery plans;

d) Ensuring network and information system security;

e) Providing regular cybersecurity training to personnel;

f) Adhering to cyber hygiene best practices.

2.21 Failure to comply with these obligations may result in a breach of Agreement and the imposition of any applicable penalties or corrective measures as defined by applicable Laws and/or the Agreement.

3 SUPPLY CHAIN REQUIREMENTS

3.1 The Supplier providing IT services and/or products is expected to meet the following security requirements to maintain protection and accountability across the supply chain:

i. The Supplier undertakes and guarantees that it will always act in accordance with applicable IT standards, laws and regulations, and that the service, as well as the Supplier's IT environment, operating environment, networks and other IT systems meet all requirements according to such applicable regulations and standards. Furthermore, the Supplier guarantees that it has the competence, capacity, and permission required, where applicable, in accordance with applicable law, to perform the service in a reliable and professional manner.

ii. The Supplier shall conduct regular security assessments of all sub-suppliers engaged in the performance of services under the Agreement. These assessments shall be conducted at least once every six months and shall evaluate the sub-suppliers' compliance with industry-standard security practices and any specific security requirements set forth by Mölnlycke. The Supplier shall document the findings of these assessments and provide a comprehensive report to Mölnlycke within 30 days of the completion of each assessment.

iii. The Supplier shall implement information security requirements for all IT products (e.g., hardware, software) or IT services (e.g., cloud services) provided to Mölnlycke. This includes ensuring secure development practices and verifying the security of sub-contracted work.

iv. The Supplier must ensure that any sub-suppliers involved in delivering IT products or services comply with the same security requirements as outlined in the Agreement. The Supplier remains responsible for ensuring compliance throughout their supply chain.

v. If the IT product includes components sourced from other suppliers, the Supplier must ensure appropriate security practices are applied. This includes ensuring that software developers, hardware providers, or third-party vendors follow secure development and handling practices.

vi. The Supplier must upon request provide a detailed list of all software components, including any open-source libraries or third-party dependencies, used in the products supplied to Mölnlycke.

vii. The Supplier shall upon request provide clear documentation of the security functions implemented in their products and offer guidance on secure configurations for their operation.

viii. Mölnlycke may validate the security of supplied products through monitoring, penetration testing, or third-party audits. The Supplier must cooperate in such assessments to ensure that security requirements are being met.

ix. The Supplier must identify and document any product or service components critical to the functionality or security of the system, especially if subcontracted. Such components will be subject to additional scrutiny and monitoring.

x. The Supplier must provide assurances that the origin and integrity of critical components can be traced throughout the supply chain.

xi. The Supplier must implement tamper prevention mechanisms for critical components and provide assurances, such as cryptographic hash verifications or digital signatures, that components are genuine and unaltered. Mölnlycke may conduct assessments to verify compliance.

xii. The Supplier must provide evidence of meeting required security levels, such as certifications under formal evaluation schemes.

xiii. The Supplier shall implement processes to manage the lifecycle and availability of IT components. This includes planning for component obsolescence and identifying alternative suppliers if components are no longer available.

xiv. The Supplier must plan for the secure disposal or transfer of IT components when they reach the end of their life cycle. This includes identifying alternative suppliers for critical components and securely managing the transition.

4 AUDIT RIGHTS

4.1 Mölnlycke reserves the right to verify the Supplier's and, where applicable, sub-supplier's compliance with the ISR. This includes the right to conduct audits, with reasonable notice and at least once per year or more frequently and unannounced in the event of suspected non-compliance, of the Supplier's premises, systems, processes, and records. Such audits may include, but are not limited to, physical inspections, interviews with personnel, and reviews of security controls, certifications, and policies. The Supplier agrees to fully cooperate during such audits and to provide all necessary access and information. Mölnlycke may issue questionnaires or request specific documents, which the Supplier must complete and return in a timely manner. If any audit reveals non-compliance, the Supplier shall promptly implement corrective actions as requested by Mölnlycke.

4.2 Audits requested by the Supplier are conducted at Supplier's cost, while audits initiated by Mölnlycke will be covered by Mölnlycke.

5 REMUNERATION

Any entitlement to remuneration regulated in the Agreement includes remuneration for the obligations under these ISR.

6 TERM AND TERMINATION

6.1 Upon termination of the Agreement, Parties shall comply with records management, return of assets, secure disposal of information, and any ongoing confidentiality obligations. The Supplier shall return or destroy all Confidential Information and Customer Data at Mölnlycke's discretion. The Supplier shall ensure handover support to another supplier or to Mölnlycke at the end of the Agreement.

6.2 Mölnlycke reserves the right to terminate the Agreement with immediate effect upon providing written notice if the Supplier fails to provide evidence of ISO 27001 (re-)certification, SOC 2 Type II reports, or any other required certification within the agreed-upon timeframe. This right to terminate also applies if the Supplier fails to meet the security standards and obligations outlined in the Agreement, including but not limited to reporting Security Incident(s), protecting Confidential Information, or complying with regulatory requirements. In such cases, Mölnlycke may terminate the Agreement without penalty or liability, and any prepaid fees for undelivered services will be refunded by the Supplier.

6.3 Should any provision of the ISR be invalid or unenforceable, the remainder of the ISR shall remain valid and in force. The invalid or unenforceable provision shall be either:

i. amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible,

ii. construed in a manner as if the invalid or unenforceable part had never been contained therein.

6.4 Regardless of the expiry or termination, for whatever reason, of the Agreement, these ISR remains in force and is applicable as long as the Supplier has access to Confidential Information.

7 CHANGES

7.1 Any amendments to these ISR must be approved in writing by both Parties and in line with the procedure as set out in the Agreement.

7.2 If either Party believes that any part of the ISR requires modification due to changes in applicable Laws or regulatory requirements, they shall notify the other Party in writing. Upon such notice:

i. The Parties shall promptly review the amendment(s) and discuss any concerns, including whether the proposed changes are unreasonable, unduly burdensome, or potentially unlawful under applicable Laws.

ii. The Parties shall negotiate in good faith to agree on and implement such changes, or alternative measures, as may be necessary to ensure continued compliance with applicable Laws or regulatory requirements, as soon as reasonably practicable.

8 GENERAL TERMS

8.1 The Supplier shall not collect, use or generate Customer Data related to Mölnlycke for any purpose other than to provide the Service(s) for which the Supplier has been engaged by Mölnlycke.

8.2 The Supplier shall assign an individual to act as the primary security liaison between the Supplier and Mölnlycke. This person shall be a trusted source at the Supplier for the distribution of passwords and other confidential security matters.