

SCHEDULE 1

Information Security Obligations and Requirements

Supplier acknowledges that Ottobock and certain of its Affiliates (for the purposes of this Schedule 1 collectively “Ottobock”) qualify as entities regulated under Directive (EU) 2022/2555 (“NIS2 Directive”) as well as under the German, in particular the Act on the Federal Office for Information Security (“BSI Act”), or, as the case may be, under the respective Member State’s implementing legislation (for the purposes of this Schedule 1, the BSI Act and any other applicable Member State’s implementing legislation collectively the “Applicable National NIS2 Act”). Ottobock is therefore subject to specific legal obligations regarding the security of its network and information systems, including the management of cybersecurity risks arising from its supply chain.

Supplier acknowledges that compliance with this Schedule 1 constitutes one of Supplier’s essential contractual obligations under the Procurement Terms and the applicable Order(s).

1. General Cybersecurity Obligations

- 1.1 Supplier will collaborate with Ottobock as required to comply with the requirements set out in the NIS2 Directive and the Applicable National NIS2 Act. This will generally require, inter alia, the implementation of an information security management system (ISMS) by Supplier, taking into account relevant industry standards and certification schemes.
- 1.2 Supplier shall implement and maintain appropriate and proportionate technical, operational and organizational measures to ensure a level of security of network and information systems appropriate to the risks posed as envisaged in Art. 21 (2) NIS2 Directive and in the Applicable National NIS2 Act, particularly Section 30 BSI Act. In any case, this shall include processes to manage risks stemming from the acquisition of (components for) network and in-formation systems that are critical for Supplier’s security of network and information systems.
- 1.3 Supplier ensures that all Services and Deliverables have been and shall be designed and developed following the principle of security by design and by default. They should achieve an appropriate level of accuracy, robustness, safety and cybersecurity, and perform consistently in those respects throughout, at least, the term of the Order or, in the case of a purchase of Services and/or Deliverables by Ottobock, throughout their lifecycle.
- 1.4 Supplier shall implement and maintain appropriate cybersecurity measures applicable to their workforce, including measures to ensure cybersecurity risk awareness, regular cyber-security training and, where appropriate, certifications and/or background checks.
- 1.5 Supplier shall notify Ottobock without undue delay, and no later than within 24 hours, upon becoming aware of any security incident that may affect the provision of the Services and Deliverables to Ottobock, or Supplier’s network and information systems or those of the Ottobock. Any vulnerabilities in the network and information systems used by Supplier to provide the Services and Deliverables shall be remedied without undue delay.
- 1.6 Supplier shall ensure that its subcontractors and suppliers, to the extent involved in providing the Services and Deliverables, are subject to equivalent contractual and technical, organizational and operational security requirements as set out in this Schedule 1.
- 1.7 Supplier shall use state-of-the art technology and industry good practices in relation to cybersecurity. Where available, Supplier shall reasonably comply with and adhere to rules, guidelines, recommendations or codes of conduct applicable to Supplier or Supplier’s Services and Deliverables provided by the competent authorities, in particular the German Federal Office for Information Security (BSI).
- 1.8 Certifications that Supplier has named as certifications that it holds during the procurement process or later (e.g. ISO 27001) shall be provided to Ottobock upon request at any time, and shall be maintained during the entire term of the applicable SoW(s) as well as the warranty period (if any).

2. Documentation and compliance

- 2.1 Supplier shall provide, upon request, sufficient documentation and evidence of its security measures pursuant to Section 1 of this Schedule 1, including audit reports, penetration test results or certifications, as applicable, and/or allow for monitoring by Ottobock.
- 2.2 Supplier shall promptly inform Ottobock of any developments that could have a material impact on its ability to effectively provide all or some of the Services and Deliverables in compliance with this Schedule 1.
- 2.3 Supplier shall accept and cooperate in regular or ad hoc audits by or on behalf of Ottobock to verify compliance with this Schedule 1. Supplier agrees that Ottobock and any auditors (internally or externally) engaged by Ottobock (hereinafter referred to as “Auditors”), shall have the right to audit the lawful use of the Services and Deliverables and the performance of this Schedule 1 once during a contractual year after giving at least two (2) weeks prior notice before the scheduled audit. The notice shall include all necessary information, including a point of contact of Ottobock, enabling Supplier to take reasonable measures to support the audit. For this purpose, the Auditors shall be entitled to demand effective and comprehensive access upon reasonable upfront notice to all data, documents, data carriers and records, databases and systems related to the access and use of the Services and/or Deliverables and the performance of the applicable Order(s) by Supplier.

3. Termination of the Services and Deliverables

Upon the Services and, as the case may be, the Deliverables have terminated, Supplier shall, at Ottobock’s choice, delete or return to Ottobock all information relating to Ottobock or Ottobock’s network and information systems obtained by Supplier in the performance of the Services and/or Deliverables.