Information Security Plan
EU Regulatory Annex

This Annex describes Infor's commitments with respect to specific requirements under applicable EU cybersecurity and data governance directives, regulations, and national implementing laws ("***Applicable Cybersecurity and Data Governance Law***"), and is incorporated, where applicable to Customer (with applicability as defined below), into Customer's agreements executed with Infor (collectively, the "***Agreements***"). In the event of any conflict or inconsistency between the terms of this Annex and any other terms of the Agreements, this Annex shall prevail.

I. GENERAL

1. DEFINITIONS

1.1 Capitalized terms used but not defined in this Annex will have the meanings provided in the Information Security Plan, located at www.infor.com/security-plan (the "ISP"). The terms "ICT Process", "ICT Product", "ICT Service", "Incidents", "Network and Information Systems", "Risk", and "Significant Cyber Threat" shall have the meaning given to them in the Applicable Cybersecurity and Data Governance Law.

2. COMPLIANCE AND COOPERATION

2.1 Infor will comply with Applicable Cybersecurity and Data Governance Laws applicable to its business and, on reasonable request, cooperate with any relevant competent governmental authority and/or Customer with respect to Infor's compliance with its obligations under the Agreement in light of Applicable Cybersecurity and Data Governance Laws. Each of Infor and Customer shall inform and alert the other against any significant change or event, difficulty, risk or information that could have an adverse effect on the ICT-Services or the performance of the Agreement (unless the sharing of such information is prohibited under Applicable Law).

3. EFFECTIVE DATE

3.1 The terms in this Annex are effective on the date that the Applicable Cybersecurity and Data Governance Law becomes effective and enforceable.

4. UPDATES

4.1 Customer acknowledges that the technical and organizational security measures described in this Annex are subject to updated requirements under Applicable Cybersecurity and Data Governance Laws and to technical progress and development, and that Infor may update or modify the measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to Customer.

5. GOVERNING LAW

5.1 This Annex is governed by and enforced in accordance with the choice of law set forth in the Agreement, unless a separate choice of law is required by Applicable Cybersecurity and Data Governance Law, in which case, for purposes of this Annex, the choice of law as so required shall control over the choice of law in the Agreement.

6. LIABILITY

6.1 Infor and Customer agree that the total liability of each party and its Affiliates (as defined in the Agreement) arising out of or in connection with this Annex, whether based on breach of contract, tort or otherwise, is, as between the parties (including Affiliates), subject to the applicable provisions on limitation of liability in the Agreement. Further, Infor shall not be liable for any violation by Customer of Applicable Cybersecurity and Data Governance Laws or a failure by Customer to comply with the competent authority's requirements.

II. NIS 2 DIRECTIVE

1. SCOPE AND DEFINITIONS

1.1 The terms and conditions set forth in Section II of this Annex apply solely to EU Customers that meet the criteria and thresholds of "important" or "essential" entities that are regulated under the NIS 2 Directive. For the avoidance of doubt, Section I is deemed incorporated to this Section II.

1.2 "**NIS 2 Directive**" means 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 EU, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, and any corresponding implementing regulations.

2. GOVERNANCE

2.1 Infor has management bodies within its security office that approve, oversee, and are responsible for the implementation of Infor's cybersecurity risk-management measures, including the ISP.

3. INFORMATION SECURITY PROGRAM

3.1 Infor has implemented and will maintain the ISP so that it: (A) is designed to: (1) ensure the security and confidentiality of Infor's Network and Information Systems; (2) protect against any anticipated threats or hazards to the security or integrity of Infor's Network and Information Systems; and (3) protect against unauthorized access to or use of Network and Information Systems; and (B) sets forth Infor's policy for responding to any Incident.

3.2 The ISP is available at: www.infor.com/security-plan.

4. CYBERSECURITY RISK-MANAGEMENT MEASURES

4.1 Infor has implemented and will maintain cybersecurity risk-management measures that:

(A) are proportionate to the risks posed to Infor's Network and Information Systems taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation;

(B) are based on an "all-hazards" approach, which aims to protect Infor's Network and Information Systems and the physical environment of those systems from Incidents; and

(C) include at least the following: (a) policies on risk analysis and information system security; (b) measures to identify any risks of Incidents, including incident handling procedures; (c) business continuity, such as backup management and disaster recovery, and crisis management; (d) supply chain security, including security-related aspects concerning the relationships between Infor and its direct suppliers or service providers; (e) security in Network and Information Systems' acquisition, development and maintenance, including vulnerability handling and disclosure; (f) policies and procedures to assess the effectiveness of Infor's cybersecurity risk-management measures; (g) basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, cybersecurity training for staff on a regular basis and raising awareness concerning cyber threats, phishing or social engineering techniques; (h) policies and procedures regarding the use of cryptography and encryption; (i) human resources security, access control policies and asset management; and (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within Infor.

5. SUPPLY CHAIN

5.1 Infor represents and warrants that the supply chain security measures implemented by Infor take into account the following criteria: (a) the vulnerabilities specific to each direct supplier and service provider of Infor; (b) the overall quality of products and cybersecurity practices of Infor's suppliers and service providers, including their secure development procedures; and, where applicable, (c) the results of any coordinated security risk assessments of specific critical ICT Services, ICT Products or ICT Process supply chains carried out by EU Member States and any competent authority.

5.2 Infor performs due diligence on its third party service providers to assess their cybersecurity risk-management measures and executes agreements with such third party service providers with substantially similar cybersecurity and data governance requirements as this Annex.

5.3 Infor shall provide reasonable evidence of such supply chain security measures within a reasonable time frame after Customer request.

6. INCIDENT RESPONSE

6.1 Infor will monitor its Network and Information Systems for unauthorized access and implement an Incident response policy that specifies actions to be taken when Infor detects or becomes aware of any Incident.

6.2 If Infor becomes aware of a Significant Incident impacting Customer, Infor shall:

(A) Notify Customer as follows:

(1) Promptly and without undue delay (and in any event within 24 hours of becoming aware of such Significant Incident): (a) notify Customer of the occurrence of such Significant Incident; and (b) provide Customer with detailed information about the Significant Incident, including the following: (i) whether the Significant Incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact; (ii) any information to determine any cross-border impact of the Significant Incident; and (iii) an initial assessment of the Significant Incident, including its severity and impact, as well as, where available, the indicators of compromise;

(2) Promptly and without undue delay, provide Customer with the following supplemented information about the Significant Incident: (a) a detailed description of the Significant Incident, including its severity and impact; (b) the type of threat or root cause that is likely to have triggered the Significant Incident; (c) applied and ongoing mitigation measures; and (d) where applicable, the cross-border impact of the Significant Incident.

(B) Investigate and conduct a reasonable analysis of the cause(s) of such Significant Incident;

(C) Provide periodic updates of any ongoing investigation to Customer;

(D) Develop and implement an appropriate plan to mitigate and remediate the cause of such Significant Incident to the extent such cause is within Infor's control; and

(E) Cooperate with Customer's reasonable investigation and Customer's efforts to comply with any notification applicable to such Significant Incident, including assisting in drawing-up any report about the Significant Incident to competent authorities.

6.3 If Infor becomes aware of a Significant Cyber Threat impacting Customer (including published Infor application vulnerabilities that meet the definition of Significant Cyber Threat), Infor shall:

(A) Promptly and without undue delay notify Customer of such Significant Cyber Threat;

(B) Provide Customer with detailed information about the Significant Cyber Threat’s impact on Customer, as known to Infor;

(C) Investigate and conduct a reasonable analysis of the cause(s) of such Significant Cyber Threat;

(D) Develop and implement an appropriate plan to remediate the cause of such Significant Cyber Threat to the extent such Significant Cyber Threat materializes and the cause is within Infor's control; and

(E) Comply with reasonable requests by the Customer to provide information about the Significant Cyber Threat for the Customer to use in its required third party notifications related to the Significant Cyber Threat, if any are required under Applicable Cybersecurity and Data Governance Laws.

7. AUDIT

7.1 Infor shall hold and maintain at least one of the following certifications and attestations related to its Cloud Services (as applicable), and Infor shall, upon written request from Customer, provide Customer proof of such certifications and/or attestations:

(1) SSAE SOC 2 Type 2 (also known as AICPA TSC 2014 Type 2)
(2) ISO 27001:2022
(3) FedRAMP

Infor shall ensure that its third party service providers hold or maintain at least one of the above certifications and attestations related to the services such third party service provider provides to Infor and/or Infor customers, or provides satisfactory alternative evidence of its cybersecurity risk management measures relative to the scope of services provided.

7.2 In addition to the audit reports described in Section 7.1 above, if requested by Customer and subject to the confidentiality obligations of the Agreement, not more than once annually, unless Customer is acting pursuant to a competent governmental authority request (in which case annual limits shall not apply), Infor will promptly respond in writing to any reasonable inquiries or questionnaires from Customer (and/or its agents) regarding the content of Infor's security program and provide reasonable evidence of its compliance with the requirements of this Annex, including generally available copies of data, documents and information related to the Services necessary to assist the Customer with its compliance with any binding request or order received from any competent governmental authority. Infor will provide the relevant information without undue delay (and in any event within the timeframe provided in the binding request or order Customer has received from the competent governmental authority).

7.3 Customer may, once per year, audit Infor's compliance with its obligations under this Annex, including auditing Infor's IT security practices and applicable control environments, in accordance with the process outlined in this Section 7, only if:

(A) Infor has not provided sufficient evidence of its compliance with the cybersecurity risk management measures described in this Annex through the reports and documentation referenced in Section 7.2 above, or, if applicable, any other audit reports or other information Infor makes generally available to its customers;

(B) A Significant Incident has occurred;

(C) Infor has notified Customer that it is subject to a government access request related to Customer Data;

(D) An audit is formally requested by a competent governmental authority with jurisdiction over Customer; or

(E) Mandatory Applicable Cybersecurity and Data Governance Law conferring Customer a direct audit right.

7.4 Before the commencement of an audit, Customer and Infor will mutually agree upon the scope, timing, duration, control and evidence requirements. Customer may use an independent accredited third party audit firm to perform the audit on its behalf, provided the third party auditor is mutually agreed to by Customer and Infor (which shall not include any third party auditors who are either a competitor of Infor or not suitably qualified or independent). Customer agrees that the audit will be conducted without unreasonably interfering with Infor's (or its subcontractors') business activities, during regular business hours with reasonable advance notice, and subject to Infor (or its subcontractors') applicable security policies and confidentiality procedures. Where on-site audits of physical data centers, systems, or facilities are not permitted, Infor will work with Customer (and its subcontractors, if applicable) to reach a mutually agreeable resolution sufficient to provide information necessary for Customer to comply with audit requirements under the Applicable Cybersecurity and Data Governance Laws. Neither Customer, nor the auditor, shall have access to any data from Infor's other customers or to Infor systems or facilities not involved in the Services provided to Customer. Customer shall provide the results of any audit to Infor. The parties shall mutually agree on any corresponding reports or remediation. Infor shall use commercially reasonable efforts to address agreed-upon remediation.

7.5 Customer is responsible for all costs and fees related to the audit, including all reasonable costs and fees Infor expends for the audit and any costs and fees Infor incurs from any subcontractor where the audit involves a subcontractor, unless such audit reveals a material breach by Infor of this Annex, in which case Infor shall bear its own expenses of that portion of the audit related to the breach.

III. DORA

1. SCOPE AND DEFINITIONS

1.1 The terms and conditions set forth in Section III of this Annex apply solely to EU Customers that meet the criteria and thresholds for financial entities regulated by DORA. For the avoidance of doubt, Section I is deemed incorporated to this Section III; specific paragraphs in Section II also apply if specifically referenced in this Section III.

1.2 "**DORA**" means the Digital Operational Resilience Act (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022.

2. SERVICES

2.1 The ICT Service provided by Infor to Customer is described in the Agreements.

3. LOCATION

3.1 For the avoidance of doubt, Customer production data is stored in the selected deployment location and Infor shall not move any of Customer's production data outside of this location without Customer's prior written approval and direction. At Customer's direction, limited amounts of personal data may be remotely accessed from outside of the selected deployment location for purposes of providing support and services to Customer. Infor shall notify customer in advance if it envisages changing the locations (i.e. the regions or countries) where the Services will be provided and where Customer Data will be stored and processed, as set out in the Agreement.

4. SECURITY PROGRAM AND SLAS

4.1 Cybersecurity risk management measures described above in Section II.3 and Section II.4 apply. Infor's incident response commitments in Section II.6 also apply. For the avoidance of doubt, Infor's insolvency is deemed added as an obligation for return of Customer Data under the ISP.

4.2 Infor's service level availability commitments are described in the Service Level Agreement at https://www.infor.com/service-level-description ("SLA"). Product-specific support commitments are described in the Order Form, if applicable.

5. ICT SECURITY TRAINING AND AWARENESS PROGRAMMES

5.1 Should Infor access Customer's on-premises network information systems as part of the Services, Customer may request Infor to participate, on reasonable notice, in any appropriate ICT security awareness programme and/or digital operational resilience training that the Customer provides or operates in connection with its business ("Training"). In this regard, the parties agree that:

(A) The frequency, timing and duration of such Training shall be agreed by the parties in advance;

(B) Infor reserves the right to recover from the Customer its reasonably and properly incurred expenses; and

(C) Infor's participation in such Training shall not require it to do anything which may interfere, prevent or impede Infor from providing the ICT Services or otherwise performing its obligations under the Agreement.

6. TERMINATION

6.1 In addition to the termination rights set out in the Agreement and elsewhere in these terms and conditions, as authorized by Art. 28 Section 7 of DORA and subject to the termination process in the Agreement, Customer may terminate the Agreement in whole or in part solely in the following cases: (i) if Infor has failed to cure a significant breach of Applicable Cybersecurity and Data Governance Laws or this Annex, (ii) if circumstances are identified by Customer that are deemed capable of altering Infor's performance of the ICT Services, including material changes that affect the Agreement or the situation of Infor, (iii) if evidenced weaknesses are found pertaining to Infor's overall ICT risk management and in particular in the way Infor ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal data or otherwise sensitive data, or non-personal data, or (iv) if the competent government authority can no longer effectively supervise Customer as a result of the conditions of, or circumstances related to, Infor or the Agreement.

7. DEALINGS WITH COMPETENT GOVERNMENTAL AUTHORITIES

7.1 Infor shall fully cooperate with competent governmental authorities and resolution authorities of Customer, including persons appointed by them.