Additional Information Security Requirements

These Additional Information Security Requirements ("AISR") supplement any other information security requirements contained within the Agreement, Novartis Third Party Code ("TPC") and Novartis Minimum Information Security Controls ("MISC").

1. Information security assessments and certifications (supplementing TPC Section 12.5)

1.1 Novartis or its nominated party may perform technical and/or other assessments including testing to evaluate security and resilience of Novartis Data and Novartis Environment.
1.2 Third Party and its subcontractors shall maintain the security certifications specified in the Agreement and audit reports.
1.3 Third Party shall ensure penetration and security tests are periodically (at least annually) performed by experienced and recognized professionals, and in alignment with Security Industry Practice on the environment where Novartis Data is processed and results from such tests are made available to Novartis upon request.
1.4 With respect to sections 1.1-1.3 above, if any gaps or vulnerabilities are found, Third Party shall without undue delay prepare and implement a remediation plan in accordance with the Security Industry Practice. Third Party's failure to comply with this requirement shall entitle Novartis to terminate the Agreement in accordance with respective Agreement's termination clause.

2. General information security requirements (supplementing MISC Section 1, 3, 5 and 6)

2.1 Third Party shall process Novartis Data in accordance with Security Industry Practice.
2.2 The information security program of Third Party shall be periodically (at least annually) reviewed and updated based on assessments addressing: (i) internal and external risks; (ii) use of defensive infrastructure or governance; (iii) the ability to detect, respond to, and mitigate threats; and (iv) the ability to fulfil regulatory requirements.
2.3 Considering relevant information security risks, Third Party shall implement adequate encryption standard(s) in line with Security Industry Practice, such as NIST 800 and/or ISO 27001 at minimum.
2.4 Third Party shall ensure multi factor authentication is in place for systems containing Novartis Data and for network access over a public data network and for access to Third Party environment (where Novartis Data is processed) from Third Party's end user workstations.
2.5 Third Party shall process Novartis Data only in: (a) a secure Production Environment; or (b) any other mutually agreed upon environment that is secure.
2.6 Third Party shall, in connection with its services, implement and maintain measures aligned to Security Industry Practice to detect, investigate, remediate, and prevent, the inclusion, implementation, or execution of any unauthorized or malicious code in any manner impacting Novartis Data or the Novartis Environment.
2.7 Third Party shall monitor available patches, evaluate, test, and implement them in a timely manner for any systems involved in processing of Novartis Data.
2.8 Third Party shall maintain adequate audit trails to support security audits and the detection and investigation of any Security Incident.

3. Continuity Standards (supplementing TPC Section 12.9 and MISC Section 2)

3.1 Third Party shall ensure the following Recovery Time Objective (RTO) and Recovery Point Objective (RPO):

Goal	Objective Maximum time for an objective [in hours]

Recovery Time Objective (RTO)	24 (or as otherwise specified in the relevant Statement of Work/Purchase Order)
Recovery Point Objectives (RPO)	24 (or as otherwise specified in the relevant Statement of Work/Purchase Order)

4. Novartis Environment (supplementing MISC Section 4, 7 and 8)

4.1 Any interface, connectivity with the Novartis Environment is subject to prior Novartis approval and may be disconnected by Novartis at any time.
4.2 If Third Party personnel receives: (i) a Novartis issued badge or similar access mechanism; (ii) a personalized Novartis network access account; (iii) a Novartis device; (iv) a Novartis e-mail account; or (v) other type of access to Novartis Environment, Third Party shall ensure that such Third Party personnel shall follow any applicable information security policies of Novartis. Third Party shall notify Novartis of any changes to the status of Third Party's personnel that may affect Novartis. Third Party shall also ensure that its personnel who may access Third Party environment containing Novartis Data will be subject to Third Partyr's monitoring on compliance with applicable Third Party information security policies and standards.

5. Security Incidents (supplementing MISC Section 12)

5.1 Third Party shall monitor, analyze, and respond to Security Incidents.
5.2 Third Party shall notify Novartis without undue delay, but not later than twenty-four (24) hours after becoming aware of Security Incident.
5.3 Novartis contact for reporting Security Incident: Phone: +420 225 775 050 (backup number: +420 225 850 012), Email: soc@novartis.com.
5.4 Third Party shall provide contact for reporting or discussing Security Incident promptly upon Novartis request.
5.5 Third Party shall, without undue delay, perform appropriate actions to minimize further exposure of Novartis Data and implement remediation actions to prevent a recurrence of a similar Security Incident.
5.6 Third Party shall report root cause and impact to Novartis Data as well as a progress of remediation actions adopted.

6. SOX requirements

6.1 For services supporting financial processing that needs to comply with Sarbanes-Oxley Act ("SOX") or Novartis financial controls, Third Party shall ensure such servicesr' information systems and related controls are assessed, at least annually, in accordance with SOX. Third Party shall be fully responsible to ensure SOX compliance and demonstrate it to Novartis. Services assessment report, such as then-current SOC 1 Type 2 or equivalent report, shall be provided to Novartis upon request. Services that shall comply with this Section shall be identified by Novartis, at its sole discretion, in the task order, SOW or in any other relevant contractual document.

7. Definitions

The definitions below apply to the capitalized terms as used in these AISR.

"**Novartis Data**" means all data, information, documents or records of whatever nature (including personal data and Novartis confidential information) and in whatever form and whether subsisting before or after the date of the Agreement and whether created or processed by Third Party in connection with the services provided to Novartis or provided by Novartis (or third parties acting on their behalf) to Third Party in connection with the Agreement.

"**Novartis Environment**" means any Novartis system or infrastructure managed by or on behalf of Novartis, Novartis Affiliates or Novartis sub-contractor accessible to Third Party.

"**TPC**" means the Novartis Third Party Code as referenced in the Agreement.

"**MISC**" means Novartis Minimum Information Security Controls as published on Novartis public internet: https://www.novartis.com/esg/reporting/codes-policies-and-guidelines and which form part of TPC.

"**Production Environment**" means an environment where the software, products, or updates are released to operations for the intended end-users.

"**Recovery point objective (RPO)**" means how much Novartis Data can be lost without possibility of recovery.

"**Recovery time objective (RTO)**" means how long the services, Novartis Data, or systems used to deliver the services, under the Agreement may be unavailable.

"**Security Incident**" means an event that actually or potentially jeopardizes the confidentiality, integrity, or availability of Novartis Data, or otherwise compromises the information security of the Novartis Environment.

"**Security Industry Practice**" means relevant industry standards and practices generally accepted within the information security community, for companies comparable to the Third Party and/or companies processing comparable information, as exemplified in various industry standards such as International Organization for Standardization (ISO/IEC) ISO/IEC ISO27001, ISO/IEC 27002:2013, SSAE-18, ISAE3402, National Institute of Standards and Technology (NIST) NIST 800-55, the Open Web Application Security Project (OWASP) Guide to Building Secure Web Applications, and the Center for Internet Security (CIS) Standards (or any generally accepted successor to such security standards) relevant for the services provided under the Agreement.