ThermoFisher SCIENTIFIC

The world leader in serving science

THERMO FISHER SCIENTIFIC
TECHNICAL AND ORGANIZATION MEASURES (TOMS)

SECTION 1. GENERAL PURPOSE & APPLICABILITY

1.1. Order of Precedence. In the event of a conflict between these Corporate Information Security Terms and Conditions, Technical and Organization Measures ("TOMs"), the relevant Service related agreement, or the Data Processing Addendum, the provision or interpretation that provides Thermo Fisher, Thermo Fisher Data, the Thermo Fisher Infrastructure, or Thermo Fisher Confidential Information stronger protection and/or rights will control.

1.2. General Purpose. Vendor provides Services that may access, create, use, process, transfer, share and/or store Thermo Fisher Data or connect to the Thermo Fisher Infrastructure. These TOMs are intended to set a minimum level of information and security protection standards and commitments which no Services can fall beneath. If Standards should fall beneath those set forth herein, or if the Vendor should fail to comply in any way with these TOMs, Vendor shall be in material breach of the Agreement.

1.3. Definitions. Annex 1 to these TOMs provides defined terms used in these TOMs. Any terms defined elsewhere in the Agreement will be given equal weight and importance as though set forth in these TOMs.

SECTION 2. SECURITY & PRIVACY GOVERNANCE

2.1 Cybersecurity Governance. The Vendor must maintain a cybersecurity program that documents the policies, standards, and controls it uses that secure the information and resources related to the Services (the "P&S Documents"). This documentation must include organizational, administrative, technical, and physical safeguards and standards appropriate to the size and complexity, the scope of the activities, and the sensitivity of the data at issue.

2.2 Human Resources Security. The Vendor must ensure that its employees, contractors, consultants, and other downstream third-party staff are regularly trained, no less than once per year. Upon request, the Vendor shall provide a certification that such training has taken place and must be able to prove that such training occurred if Thermo Fisher so requests.

2.3 Statutory / Regulatory / Contractual Compliance. The Vendor must maintain a process to be aware of and be compliant with all applicable statutory, regulatory and contractual compliance requirements. Examples include but are not limited to PCI-DSS, HIPAA, SOX, GDPR, and GLBA. Upon request, the Vendor must be able to demonstrate that compliance to either Thermo Fisher or any regulatory body.

2.4 Audit Rights. The Vendor agrees that Thermo Fisher will have the right at its expense, during normal business hours and with reasonable advance notice, and in any event, not less than twenty (20) business days or, in the event of the occurrence of any Security Incident, not less than five (5) business days to audit Vendor's compliance with these TOMs under standards established by an authorized or recognized standard setting organization (such as the International Auditing and Assurance Standards Board, Statement on Standards for Attestation Engagements (SSAE) No. 18 (SOC 1, 2, or 3)).

The Vendor agrees to conduct, upon Thermo Fisher's request, an audit by a third-party of its internal cybersecurity and data privacy compliance. The audit results will be supplied to Thermo Fisher within thirty (30) days of receipt of those results. Within sixty (60) days of the audit results, the Vendor will provide Thermo Fisher with a mitigation plan to address any risks, threats, concerns, or areas of non-compliance identified in the external audit.

SECTION 3. INFORMATION GOVERNANCE

3.1 Asset Management (AST). The Vendor must use a reasonable standard of care in maintenance of an asset inventory and classification to manage the essential information about hardware, software, and data flows/extracts/interfaces

(e.g., unique identifiers, version numbers, data recipients, physical locations). The Vendor must implement asset management controls for any assets that may be used to access Thermo Fisher Data, Thermo Fisher Infrastructure or Thermo Fisher Resources. All reliable and approved hardware and software must follow the required security standards of these TOMs.

3.2 Confidentiality. The Vendor agrees to maintain Thermo Fisher Confidential Information in all forms (including paper and electronic) in strictest confidence, using measures not less stringent than those the Vendor uses for its own most confidential or sensitive information. Notwithstanding the foregoing, in order to protect Thermo Fisher Confidential Information, Vendor will, at a minimum, use a reasonable standard of care applicable to the type of information at hand, and no less than the measures identified in these TOMs.

3.3 Access Control. The Vendor must restrict access to Thermo Fisher Data and Thermo Fisher Infrastructure to only authorized individuals. This must be enforced accordingly to ensure that (1) only authorized individuals are permitted access to business applications, systems, and networks and computing devices; (2) access to systems can be related to specific individuals; and (3) user privileges are scoped to the minimum permission required to complete their assigned duties.

3.4 Passwords. The Vendor must ensure that unique passwords are generated and regularly reviewed on a periodic basis. All passwords must remain confidential and not shared between the Vendor, its employees, contractors and third-party users.

3.5 Multi-factor Authentication. The Vendor must ensure that multi-factor authentication, or equivalent security measures, is implemented for accounts with access to internet facing Thermo Fisher Data and Thermo Fisher Infrastructure. The Vendor agrees to multifactor authentication methods that meet industry standard criteria, as defined by NIST 800-63b.

3.6 Physical Location of Data. The Vendor is responsible for notifying Thermo Fisher, in writing, before relocating any physical storage location of Thermo Fisher information to a country different from the one(s) documented in the Vendor's statement of work, contract, or Data Processing Addendum, so that any potential privacy or security implications can be addressed.

3.7 Virtualization & Cloud Solutions. If the Vendor utilizes a cloud solution, the Vendor must adhere to the same security principles required by these TOMs, the Cloud Security Alliance guidance, and applicable government regulations, laws, or directives as used throughout the Vendor's enterprise. The geographic location of the provider infrastructure resources must be made in writing to Thermo Fisher prior to transferring any of Thermo Fisher information to that provider. At all times under these TOMs, the Vendor is required to receive prior approval of Thermo Fisher, who has sole control over the data location in any cloud services to ensure compliance with local laws that restrict the cross-border flow of data.

3.8 Physical Protection. The Vendor must actively manage the physical Security Controls and ensure all buildings throughout the Vendor's enterprise that house critical IT functions (e.g., data centers, network facilities, and key user areas) and store, process or transmit Thermo Fisher Data or any other Service-related Thermo Fisher information are physically protected from unauthorized access. These physical Security Controls should follow security best practices, such as ISO/IEC 27002 requirements. The Vendor must maintain and record facility access logs with access restricted to only those personnel with a business need. At least once per quarter, these access lists must be reviewed and updated.

SECTION 4. NETWORK MANAGEMENT

4.1 Host System Configuration. The Vendor must configure host systems according to an industry standard, which include but are not limited to the following standards: Center for Internet Security (CIS); US Department of Defense Secure Technical Implementation Guides (STIGs); and OEM best practices (e.g., Microsoft, VMware, Oracle, etc.). Systems

must be configured to function as required and to prevent unauthorized actions. Upon request of Thermo Fisher, the Vendor agrees to provide a list of the standards used to configure the host systems.

4.2 Event Logging. The Vendor must use a reasonable standard of care in logging key security-related events, including but not limited to: (1) all actions taken by any individual with root or administrative privileges; (2) access to all audit trails; (3) invalid logical access attempts; (4) all individual user accesses to cardholder data; (5) use of and changes to identification and authentication mechanisms, including but not limited to creation of new privileged accounts and elevation of privileges, and all changes, additions, or deletions to accounts with root or administrative privileges; (6) initialization, stopping, or pausing of the audit logs; and (7) creation and deletion of system-level objects. Upon request by Thermo Fisher, the Vendor shall provide evidence of such event logging.

4.3 System Network Monitoring. The Vendor is required to develop and implement a process to review log alerts and security events daily for all system components to identify anomalies or suspicious activity.

4.4 Network Controls. The Vendor must ensure that all data and communications networks are secured to ensure the transmission of data is kept confidential. The Vendor shall: (1) disable or remove applications, ports, services, and similar access points installed on a computer or network facility, which are not specifically required for any business functionality; (2) ensure that network segments connected to the Internet are protected by a firewall which is configured to secure all devices behind it; (3) network segmentation is maintained to ensure that Thermo Fisher Data and any other Thermo Fisher information is isolated from non-Thermo Fisher data, both logically or physically, unless approved in writing by the Thermo Fisher Coordinator; (4) user connection capability is documented with regard to messaging, electronic mail, file transfer, interactive access, and application access; (5) all production servers are located in a secure, access-controlled location; and (6) firewalls are configured properly to address all reasonably-known security concerns. The Vendor must ensure that all infrastructure diagrams, documentation, and configurations remain up to date, controlled and available to assist in issue resolution.

4.5 Remote Access. Remote access to a network containing Thermo Fisher Data or access to the Thermo Fisher Infrastructure must be done via a secure connection (e.g., VPN). All extranet connectivity into the Thermo Fisher Infrastructure must be through Thermo Fisher-approved and authorized secure remote connections.

4.6 Malware Controls. The Vendor must implement and manage enterprise-wide detection, prevention and recovery controls to protect against malware that includes procedures and assigned responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks. At all times during the provision of any Services, the Vendor shall make reasonable efforts to ensure that all Services do not contain malicious software or malware.

4.7 Vulnerability & Threat Management. The Vendor must ensure a vulnerability management program exists to eliminate vulnerabilities and threats that could be exploited by malware or other technical methods (e.g., exploitation through technical vulnerabilities).

4.8 Testing. The Vendor should use a reasonable standard of care in ensuring that all elements of a system (e.g., application software packages, system software, hardware, and services) are tested, at least three (3) times, with a verifiable history of vulnerabilities being remediated after each scan, before the system is promoted to a production environment. All testing must be documented, and those documents must be retained for a minimum of five (5) years unless a longer period of time is required by applicable law.

4.9 Secure Destruction. The Vendor must ensure methods of destruction are formally implemented, based on the type of media, including physical, paper-based media; physical, digital media; and electronic, digital data. The Vendor must ensure that sensitive information is securely destroyed and maintain documentation of such destruction. Upon request, the Vendor shall provide Thermo Fisher (or a Thermo Fisher data subject with Thermo Fisher approval) with certification of secure destruction.

SECTION 5. SECURITY INCIDENT MANAGEMENT

5.1 Incident Management. The Vendor must maintain a documented cybersecurity event management process that covers incident response, escalation, and remediation of cybersecurity events and incidents, including as set forth herein. All such documentation must be retained for a minimum of five (5) years following the conclusion of any Security Incident, unless otherwise required by applicable law.

5.2 Reporting Security Incidents. The Vendor must notify Thermo Fisher immediately, and in any event, no later than (a) forty-eight (48) hours; (b) within any regulatory reporting requirement; or (c) as mutually agreed upon (whichever is more restrictive) after becoming aware of a Security Incident, by email to: soc@thermofisher.com, and provide information about such Security Incident sufficient for Thermo Fisher to assess the Security Incident, including any potential legal notification obligations, including without limitation, the information set out in Section 5.2.1 below.

5.2.1 Initial Notification. The notification of a Security Incident must include to the extent then available: (a) the date the Security Incident occurred; (b) the date the Security Incident was discovered; (c) the nature, scope and root cause of the Security Incident; (d) the attack vector (if relevant) and timeline of the Security Incident; (e) the Thermo Fisher Data involved in the Security Incident, including what personal information, if any, was or may have been affected; (f) the number and identity of affected individuals whose personal information may have been affected; (g) all provided or planned notifications of the Security Incident to any data subject, service provider, employee, regulatory body or governmental authority, law enforcement, insurer, or other third party; (h) the steps Vendor has taken to investigate the Security Incident; (i) the identity of any outside forensic or other consultants assisting the Vendor in investigating or responding to the Security Incident; and (j) remediation plan to prevent recurrence (the "Initial Notification").

5.2.2 Updates. Following the Initial Notification, the Vendor must provide to Thermo Fisher regular and timely updates, including providing, as it becomes known, any information set out in Section 5.2.1 that was not included in the Initial Notification, and any other information Thermo Fisher may request relating to the Security Incident to assess and comply with its own legal obligations or for its own business purposes.

5.2.3 Final Report. Upon completion of the Vendor's investigation of a Security Incident, the Vendor must provide Thermo Fisher with a full accounting of the Security Incident, including without limitation final information on the items set out in Section 5.2.1 above.

5.2.4 Additional Requirements. Thermo Fisher may impose additional or revised notification requirements based on applicable state breach notification laws or requirements under applicable domestic and/or international privacy laws.

5.3 Cooperation. The Vendor must fully cooperate with Thermo Fisher in the event of a Security Incident and take steps as directed by Thermo Fisher to assist in the investigation, mitigation, and remediation of the Security Incident. Such cooperation shall include, without limitation, the Vendor making available to Thermo Fisher, promptly upon request, direct access to the person leading the forensic investigation into the Security Incident and providing documentation and information relating to the Security Incident as requested. In the case of noncooperation, Thermo Fisher may terminate the agreement with the Vendor without penalty.

5.4 Notifications. Thermo Fisher shall make the final decision how, when, and whether to notify any third parties of any such Security Incident, including data subjects, employees, service providers, law enforcement, regulatory bodies, or governmental authorities, and/or the public of any such Security Incident. The Vendor must not inform any third party of any Security Incident to the extent that it may be associated with or linked to Thermo Fisher without first obtaining Thermo Fisher's prior written consent. Further, the Vendor agrees that Thermo Fisher shall have the sole right to determine the contents of any such notice of a Security Incident and whether to offer identity theft protection services or other services to affected individuals, if any. Notwithstanding anything herein to the contrary, in the event that the Vendor is required by law to provide a notification or communication to a third party or government entity, the Vendor must provide Thermo Fisher at least seventy-two (72) hours advance notice of the form and content of the intended

communication to: soc@thermofisher.com and must provide Thermo Fisher with the opportunity to revise and approve the final communication.

5.5 Data Backups. The Vendor must ensure that backups of essential information and software, and in particular any critical data related to Thermo Fisher Data, are performed on a regular basis, according to a defined cycle in accordance with the Vendor's internal policies and industry best practices. The Vendor shall establish alternate and/or separate storage sites to ensure Availability and accessibility of Thermo Fisher Data. The Vendor shall regularly test the backup process, at least once per quarter.

SECTION 6. THIRD-PARTY MANAGEMENT

6.1 Outsourcing. The Vendor must operate a formal process to address due care and due diligence considerations in the selection and management of downstream third-party vendors/processors/suppliers. The Vendor maintains all the necessary agreements with all third-parties that specify the security and data privacy requirements to be met before commencing work on behalf of the Vendor that could have an impact on Thermo Fisher Data, the Thermo Fisher Infrastructure, or any of Thermo Fisher's business operations with the Vendor. The Vendor shall ensure that these agreements align with the Security Requirements of these TOMs. The agreements between the Vendor and these third parties expressly require the approval of the Vendor prior to any additional subcontracting activities.

6.2 Indemnification. In addition to any other indemnification, reimbursement, or defense obligations set forth in the agreement or terms to which these TOMs are attached, the Vendor must defend, indemnify and hold Thermo Fisher and its affiliates and its and their respective officers, directors, employees and agents harmless from and against any and all losses, claims, actions, proceedings, judgments, expenses, damages and liabilities (including, without limitation and regardless of outcome, attorneys' fees and court costs) arising out of or resulting from (i) any breach of these TOMs or (ii) any Security Incident.

6.3 Notification Related Costs. The Vendor's obligations to indemnify Thermo Fisher and its affiliates will include without limitation Notification Related Costs (defined below) incurred by Thermo Fisher and its affiliates arising out of or in connection with a Security Incident. "Notification Related Costs" means and includes any internal and external costs, whether incurred by Thermo Fisher or a third party, associated with addressing and responding to a Security Incident, including, but not limited to: (a) analysis of potential notification obligations and notification planning; (b) preparation and mailing or other transmission method; (c) preparation and mailing or other transmission of such other communications to data subjects, employees, service providers, law enforcement, regulatory bodies or governmental authorities, and/or the public as Thermo Fisher deems appropriate; (d) establishment of a call center or other communications procedures in response to such Security Incident; (e) public relations and other similar crisis management services; (f) legal, forensic, investigation, and accounting fees and expenses associated with Thermo Fisher's investigation of, response to, and remediation of such Security Incident; (g) communication with and responses to insurers; (h) costs for credit monitoring and identity protection services; and (i) costs associated with any communications with customers, regulators, individuals, employees, or others relating to the Security Incident.

6.4 Limitation on Liability. Notwithstanding anything to the contrary in the agreement or terms to which these TOMs are attached, no provision shall limit the liability of the Vendor nor exclude any types of damages recoverable with respect to any claims arising out of these TOMs, including with respect to Notification Related Costs for a Security Incident.

ANNEX 1
DEFINITIONS

The following defined terms are used in this Exhibit and have the meanings set forth below. Any terms defined elsewhere in the Agreement will be given equal weight and importance as though set forth in this Annex.

The following defined terms are used in these TOMs and have the meanings set forth below.

"**Availability**" means ensuring timely and reliable access to and use of information.

"**Confidential Information**" means any information that during the Term is disclosed by or on behalf of a Party or its Affiliate (the "Disclosing Party") to the other Party or its Affiliate (the "Receiving Party") and at the time of disclosure: (i) is designated in writing as confidential or proprietary; (ii) is designated orally as confidential or proprietary, and embodied by the Disclosing Party in written or other tangible form, including meeting minutes, memos, diagrams, flow charts, and software; or (iii) should reasonably be understood by the Receiving Party to be confidential to the Disclosing Party under the circumstances.

"**Confidentiality**" means preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.

"**Security Incident**" means any (a) actual, reported, or suspected loss of, or unauthorized disclosure, destruction, alteration, use of, or access to, Thermo Fisher Data or the Thermo Fisher Infrastructure; (b) act or omission that compromises the administrative, technical, or physical safeguards (including these TOMs) designed to protect the security, confidentiality, availability, or integrity of Thermo Fisher Data or the Thermo Fisher Infrastructure; or (c) event that disrupts the operations of systems relating to the provision of services to Thermo Fisher or its affiliates or impacts Thermo Fisher Data or the Thermo Fisher Infrastructure. For clarity, and not by way of limitation, Security Incident includes any such incident reported to Vendor by a service provider, supply chain partner, or other third party.

"**Services**" mean all necessary or required services, tasks, functions, products and other responsibilities and activities as set forth in, or reasonably inferable from, the Agreement, or any Scope of Work, Order or any such other written document.

"**Thermo Fisher Data**" means (a) all data and information Thermo Fisher provides to Vendor, made accessible by Thermo Fisher to Vendor, or to which Vendor has access or that Vendor (or Vendor Services) retrieves or collects during the course of performance of the Services, including without limitation data and information from customers of Thermo Fisher; (b) all archives, derivatives, summaries, abstracts, compilations, combinations with other information, modifications or manipulations of the foregoing data or information, aggregated information, de-identified information, data sets, subsets, and the like related to, or derived from such data or information; and (c) all reports generated by the Services, or otherwise generated or provided by Vendor relating to or in connection with the Product or Services.

"**Thermo Fisher Infrastructure**" means any information technology system, virtual or physical that Thermo Fisher or its Affiliates own, control, lease, or rent, and that resides on or outside the Thermo Fisher Network. Thermo Fisher Infrastructure includes infrastructure obtained from an IaaS provider and systems that are provided and located on the Thermo Fisher Network as part of a Service.