GLOBAL SECURITY ADDENDUM

Overview: PerkinElmer Informatics, Inc. (together with its affiliates, "**PerkinElmer**") has designed this Global Security Addendum ("**Security Addendum**") to protect the confidentiality, security, and availability of Customer Data, taking into account the type of Service being provided, the resources available to PerkinElmer, the nature of Customer Data being input into the Services, and PerkinElmer's commitment to protecting the security and confidentiality of such Customer Data. All capitalized terms not otherwise defined herein shall have the meanings ascribed to them in Customer's Software as a Service License Agreement ("**SaaS Agreement**"). This Security Addendum is subject to change at PerkinElmer's discretion, provided that such changes will not result in a material reduction in the security level of the Service provided during the purchased subscription term.

Security Practices

PerkinElmer is responsible for implementing and maintaining the technical, process, and organizational security measures in relation to the Service set forth in this Security Addendum. Customer remains the primary account and system administrator and is responsible for security, maintenance, and appropriate protection of Customer Data by (i) selecting and purchasing appropriate Service(s), (ii) implementing appropriate identity, encryption and logical access controls, and (iii) implementing and ensuring compliance with any Customer-specific security measures implemented by Customer for the use of the Service by its Users. Certain PerkinElmer services may be available to help Customer meet these requirements. Customer may contact its PerkinElmer Sales Account Representative for further details.

Physical Security

PerkinElmer utilizes public cloud infrastructure, including Amazon Web Services and/or Microsoft Azure, as third-party service providers in connection with its provision of the Service. The following physical security controls apply to the Service, and may, as applicable, be performed by PerkinElmer's third-party service providers:

a) PerkinElmer's third-party service providers provide the servers utilized in PerkinElmer's provision of the Service, are responsible for the physical security of the data centers, and are either SSAE18-SOC 2 Type 2 certified or have been reviewed by PerkinElmer to ensure conformance by such service provider to the requirements of the Trust Services Criteria (as defined below).
b) PerkinElmer's third-party hosting providers are required to maintain controls and periodically review access to the data centers utilized by PerkinElmer, including, but not limited to, controls such as badge access and video monitoring. PerkinElmer additionally reviews and monitors physical access control enforcement, using SOC2 audit reports.

Security Controls Audit and Reporting

PerkinElmer will engage qualified third-party auditors to perform annual examinations of its systems and processes related to the Service in accordance with the Trust Services Criteria of Security, Availability, and Confidentiality published by the American Institute of Certified Public Accountants ("Trust Services Criteria").

A PerkinElmer SOC2 report or equivalent report (as determined by PerkinElmer) may be available to Customer upon Customer's request, subject to PerkinElmer's report distribution requirements. Any report provided by PerkinElmer to Customer shall be deemed PerkinElmer Confidential Information and subject to the confidentiality obligations set forth in the SaaS Agreement or other confidentiality agreement entered into by and between the parties, as applicable.

Administrative controls

Screening

Where permitted under applicable law, PerkinElmer will perform pre-employment criminal background screening on employees and contractors who have access to Customer accounts.

PerkinElmer Access

PerkinElmer will restrict access to Customer accounts to its employees, contractors, and agents who require access for the sole purpose of providing the Service (including the provision of professional and technical support services during

the subscription term), subject to need and least privilege principles. PerkinElmer personnel who access the Service will be required to log on using an assigned username and password and are required to complete appropriate security, data classification, and privacy training. Further, administrative access granted to employees, contractors, and agents will be reviewed periodically to determine the appropriateness of access based on his or her role and relationship with PerkinElmer.

Customer Access
As the primary administrator of the Service, Customer is responsible for the management of its end user accounts, including creation, change management and termination, and enforcement of related remote working and password control policies. Access to the application and Customer Data are controlled by use of login/password mechanisms as applicable to the Service purchased by Customer.

Data Security
PerkinElmer has adopted generally recognized industry standard practices to secure Customer Data in transit and at rest.

Monitoring
PerkinElmer has adopted generally accepted industry practices to monitor security, confidentiality, availability, and performance of the Service. PerkinElmer implements appropriate audit logging and event monitoring capabilities conforming to the requirements of the Trust Services Criteria, including protection of systems audit tools, network security, and monitoring systems use. Audit logs are retained in a manner designed to prevent unauthorized access, use, alteration or destruction.

Customer Data Management and Return
The Service enables Customer to retrieve (by exporting or archiving) and delete Customer Data. Depending on the purchased Service, Customer may not have access to the Service or Customer Data during a suspension of Services or following the expiration or termination of the Service subscription term. Except as otherwise set forth in the SaaS Agreement, Customer is responsible for retrieving a copy of its Customer Data prior to the expiration or termination of the Service, and PerkinElmer may delete Customer Data following the expiration or termination of the subscription term in accordance with the terms of the SaaS Agreement. The Customer Data retrieval capabilities described herein are not back-up capabilities and are not intended to restore Customer's Service to its state at a prior point in time. Disaster recovery and back-up capabilities are described in more detail below.

Disaster Recovery Capabilities
PerkinElmer will provide disaster recovery capabilities to restore the Service in the event the Service is completely down. Customer Data images are created for disaster recovery purposes only. Customer Data will not be backed up or recoverable by PerkinElmer on a Customer-by-Customer basis during the subscription term unless this capability is separately purchased by Customer. Any Customer requiring this capability should contact their PerkinElmer Sales Account Representative to discuss available services.

"Recovery Point Objective" or "RPO" means the maximum acceptable level of data loss following an unplanned event, such as a disaster (natural or man-made), act of crime or terrorism, or any other business or technical disruption that could cause such data loss. The RPO represents the point in time, prior to such an event or incident, to which lost data can be recovered (given the most recent backup copy of the data). PerkinElmer's RPO is 24 hours.

"Recovery Time Objective" or "RTO" means the period of time within which Service must be restored following an unplanned event or disaster. PerkinElmer's RTO is 48 hours.

Reports of and Response to Security Breach
In the event of a material breach of the security of the Service which results in unauthorized access to Customer Data, subject to and in accordance with applicable law, PerkinElmer will (i) promptly notify Customer of such breach in writing (including by e-mail to a designated point of contact) as soon as reasonably practicable after becoming aware of such breach, (ii) promptly provide to Customer upon request relevant information and documentation available to it

regarding such unauthorized access, and (iii) upon request by Customer, grant Customer the right to audit the forensic evidence provided by PerkinElmer using a third-party auditor reasonably acceptable to PerkinElmer. PerkinElmer shall be under no obligation to notify Customer of routine security alerts in respect of the Service (including, without limitation, pings and other broadcast attacks on firewalls or other devices).

Last Updated: September 23, 2020