Information Security Exhibit

Data security sits at the foundation of product development at UiPath (hereinafter, "**UiPath**"). This Information Security Exhibit ("**Exhibit**") points out the organizational policies and controls at UiPath that are aimed at maintaining confidentiality, integrity, and availability of Customer Data used with UiPath Software and/or Services. Unless defined herein, capitalized terms will have the meaning given to them in the applicable agreement executed between UiPath and Customer with respect to access to, and/or use of, paid Software and/or Services ("**Agreement**") and incorporates this Exhibit, and the collection of documents and policies made available and amended by UiPath from time to time on the Trust Portal at uipath.com/legal/trust-and-security (or successor website).

"Customer Data" means any data, information, and proprietary Customer content created prior to or independently from any Customer interaction with the Software and imported into the Software, or accessed by UiPath in connection with, or for the purpose of, provision of any Services. Customer Data may contain Personal Data.

"**Security Incident** "means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data processed by UiPath for the purposes of the Agreement.

"**WorkFusion Products"** means the intelligent automation software products originally developed and offered by WorkFusion, Inc. (acquired by UiPath) and made available by UiPath as part of its software portfolio.

1. SCOPE

1.1. This Exhibit highlights security measures maintained by UiPath, with respect to its internal infrastructure and its Software, that impact the confidentiality, integrity, and availability of Customer Data. This Exhibit does not cover any standards maintained by providers of Third-Party Services, and, unless otherwise set out in this Exhibit, UiPath does not make any commitment in respect of Third-Party Services.

1.2. Information on the standard security requirements imposed on UiPath providers that may have access to Customer Data can be found at https://www.uipath.com/assets/downloads/cybersecurity-requirements (or successor website).

2. SECURITY CERTIFICATIONS AND ATTESTATIONS

2.1. UiPath recognizes the importance of implementing appropriate technical, organizational measures and security controls to prevent unauthorized access, disclosure, alteration, or destruction of Customer Data. UiPath maintains a comprehensive information security management system and engages independent auditors to provide industry standard certifications and attestations (collectively "**Security Certifications and Attestations**"). Further information is available on the UiPath Trust Portal and Trust Center (trust.uipath.com), including the UiPath Customer Shared Responsibility Guide, and may also be provided upon Customer's written request. A list of the Security Certifications and Attestations is available below:

a) ISO/IEC 27001 certification - information security management system (ISMS)

b) ISO/IEC 42001 certification - AI management system (AIMS)

c) ISO 9001 certification - quality management system (QMS) fundamental to UiPath's secure software development lifecycle (SDLC)

d) SOC 2 Type 2 + C5 attestation

e) SOC 1 Type 2 attestation

f) HIPAA Type 2 attestation

g) Cyber Essentials Plus certification

h) AIUC-1 certification - standard for AI agent security, safety and reliability

2.2. UiPath is constantly working to improve its quality and security standards and is working on an internal roadmap of certifications, attestations and standards relevant and adequate for the industry in which UiPath operates. UiPath shall not modify the level of security measures provided in this Exhibit during the term of the Agreement, to decrease the capabilities, functionality, or operation of the Software.

2.3. WorkFusion Products are part of the UiPath family of products but may have different levels of security measures and different configurations or attestations. Unless expressly identified in the relevant certification attestation, WorkFusion Products shall not be deemed included within the scope of the Security Certifications and Attestations above. ISO/IEC 27001 certification and SOC 2 Type 2 attestation relating to WorkFusion Products shall be made available upon Customer's request. Vendor Risk Management, Incident Management, and Business Continuity measures may vary from UiPath's standard framework across WorkFusion Products or service offerings to reflect differences in architecture, delivery model, and operational requirements, provided that the measures applied to the applicable product or service are consistent with reasonable industry standards.

3. PRODUCT SECURITY

3.1. Product Development Practices

3.1.1. UiPath follows a secure software development lifecycle ("**SDLC**"). The SDLC process is enforced for every release and includes code reviews, threat modeling during service design and security assessments such as static and dynamic code analysis, open-source software assessments, manual penetration testing, and bug bounty programs.

3.1.2. UiPath follows change control procedures to manage changes to information systems, supporting infrastructure and facilities. Prior to implementing any changes, UiPath will (1) establish internal acceptance criteria for production change approval and implementation; and (2) require internal stakeholder approval prior to change implementation as applicable.

3.1.3. UiPath tests system and application changes, including relevant security controls as applicable. System and application changes must meet defined acceptance criteria prior to implementation.

3.1.4. Additionally, UiPath restricts and tracks personnel access to program source code and requires developers to periodically attend secure system development training.

3.2. Cryptographic Controls

3.2.1. An important part of UiPath security strategy is encryption, aimed to prevent information from being accessed unlawfully. Customer Data is encrypted at rest in any data store that is part of the Software. Customer Data is transmitted over protected channels, whether it travels over the internet or within UiPath internal service components. Customer has the flexibility to configure the encryption of certain installed Software, under customer-managed key (CMK), as detailed in the relevant Documentation.

3.2.2. Only industry-standard algorithms for encryption and key strength that are approved by UiPath engineering and IT departments are used to encrypt data and assets used in production or business use-cases. UiPath uses encryption to protect UiPath and Customer or third-party non-public data in transit across public networks.

3.2.3. Additionally, encryption is used to protect UiPath and Customer or other third-party data at rest over which UiPath has custodianship. UiPath uses known Certificate Authorities for the issuance of public key certificates. Keys have defined activation and deactivation dates, so they can only be used for a limited period, and keys are protected from modification, loss, destruction, and unauthorized disclosure during their lifecycle (use, storage, and handling).

3.3. Network Security and Operations

3.3.1. All the web services offered as part of Software are enabled for TLS 1.2+, by default and by design.

3.3.2. Intrusion prevention and detection systems, secure gateways, and firewalls are in place to protect UiPath

network infrastructure supporting the Software. Separation of test, development and production environments is ensured. Regular backups of essential business information are maintained through cloud providers for Cloud Software. An appropriate backup cycle is used and documented. Event logs, recording user activities, exceptions, faults, and information security events are produced, kept, and regularly reviewed.

3.3.3. Information about technical vulnerabilities of information systems being used is assessed in a timely fashion, and appropriate measures are taken to address the associated risk in line with UiPath's exposure to such vulnerabilities.

3.4. Software Access Controls

3.4.1. UiPath has built access control features into its Software which Customer can utilize to provision, de-provision and authorize its own users. Details can be found in the relevant Documentation.

3.5. Access to Customer Data

3.5.1. UiPath does not have access to Customer Data used by Customer with On-Premise Software unless access is expressly granted by Customer.

3.5.2. UiPath personnel may have access to Customer Data used by Customer with Cloud Software solely for the purpose of fulfilling UiPath rights and obligations under the Agreement. UiPath leverages privileged identity management to minimize granting access to UiPath personnel to Customer Data in Cloud Software. UiPath personnel who need to edit system resources, access, or modify Customer Data must use privileged identity management to temporarily raise their access level. Privileged identity management requests must be accompanied by a valid reason for access. The activity conducted while using privileged identity management is logged and recorded.

3.5.3. Unless otherwise agreed by Customer and save for the data sub-processors listed on the Trust Portal, UiPath shall restrict third party access to Customer Data.

3.6. Tenant Data Segregation

3.6.1. Data at rest from each tenant of the Cloud Software is logically segregated. UiPath provides the necessary mechanisms to enable tenants to enforce access and authorization controls for users, as they access data inside the Software.

3.7. Customer Data Hosting

3.7.1. As part of Cloud Software, UiPath may use third-party service providers which may process Customer Data. UiPath will keep said third party service providers to confidentiality obligations and adequate measures for the security of Customer Data consistent with those provided for UiPath in this Exhibit. A list of third-party service providers, as amended from time to time, is maintained on the Trust Portal.

3.7.2. Customer shall be able to consult any details around data residency (location availability, tenancy per different UiPath products etc.) on the following dedicated page https://docs.uipath.com/automation-cloud/automation-cloud/latest/admin-guide/data-residency-cloud (or successor website).

3.7.3. In case of a conflict between the terms of this Exhibit and the data processing agreement between Customer and UiPath, the applicable data processing agreement shall prevail.

3.8. Customer Data Backups

3.8.1. Regular backups of Customer Data in Cloud Software are performed automatically by UiPath underlying infrastructure as a service/platform as a service ("**IaaS/PaaS**") provider. Each backup is stored in multiple locations to ensure resiliency.

3.8.2. Customer may notify UiPath in writing with sufficient time in advance to obtain the available backup records stored by UiPath to review any record of system activity related to Customer Data.

3.9. Customer Data Retention

3.9.1. As a standard, Customer Data is kept for the duration of the Agreement. Following termination of the Agreement and upon express written instructions from Customer, UiPath will ensure that Customer Data will be, as requested by Customer in the timeframe specified by the applicable law, deleted, or returned to Customer either manually or, if technically available, via direct export from the relevant Cloud Software.

3.10. Logs Information

3.10.1. Logging capabilities are built into the Software, which Customer can enable to capture informational events, errors, and warning messages relevant to the application as well as audit trails for actions performed. Details can be found in the Documentation.

3.10.2. UiPath enables operational logs and security logs of activity in Cloud Software. Operational logs are used to monitor uptime and availability of infrastructure and Cloud Software. Security logs are used to identify Security Incidents, policy violations, fraudulent activity, auditing, and forensic analysis, to support investigations, establish baselines, and identify trends and potential long-term problems.

3.10.3. UiPath shall generate administrator and security event logs for systems and applications that store, allow access to, or process Customer Data. Such administrator and security event logs shall be archived for a minimum of one hundred eighty (180) calendar days.

3.11. Personal Data Protection

3.11.1. Rights and obligations between UiPath and Customer with respect to protection of Personal Data that is part of Customer Data are governed by appropriate data protection agreements signed by the parties, or in lack thereof, the data protection agreement available on the Trust Portal.

3.11.2. UiPath takes Personal Data protection very seriously and encourages Customers to minimize the use of Personal Data with Cloud Software or during provision of support or professional services, in line with the principles of applicable law and industry best practice.

3.11.3. UiPath is committed to providing a secure operating environment; however some Software components might not meet all standards required by industry standards such as PCI DSS, or HIPAA. UiPath expressly prohibits Customers from using CHD, SAD, PHI, or any other specifically regulated personally identifiable information with Cloud Software and when engaging UiPath for support or professional services, except where UiPath has expressly permitted otherwise in the Documentation, this Exhibit or the Trust Portal. Nonetheless, Customer is ultimately responsible in deciding whether the Software can be used in accordance with the laws, rules, and regulations applicable to Customer's operations.

3.11.4. Notwithstanding anything in this Exhibit, Customer is ultimately responsible in deciding whether UiPath's Software and/or Services can be used in accordance with the laws, rules, and regulations applicable to Customer's operations.

3.11.5. UiPath may make available products or features in early access, preview, research that are not part of the generally available commercial offering and that may be subject to reduced or different security standards and controls, and Customer is required to limit or exclude the processing of personal data or other confidential or sensitive data in connection thereof.

3.11.6. As data controller, UiPath processes Personal Data in accordance with the privacy policy available on the Trust Portal. UiPath will give notice to Customer of any data subject access request received by UiPath but to which Customer is due to respond, as data controller.

3.12. Malware

3.12.1. UiPath performs regular testing of first party and third-party code included in Software.

3.12.2. UiPath deploys, maintains, and updates anti-malware protection within its operating environment and on corporate computing resources.

3.13. Vulnerabilities Management

3.13.1. Vulnerabilities identified in the Software are mapped to industry-standard Common Vulnerability Scoring System ("**CVSS**") methodology (i.e., critical, high, medium, and low). Identified vulnerabilities shall be remediated in a timely manner within internally defined timeframes.

3.13.2. Regular testing is also performed directly against the Software, and UiPath has a bug bounty program that aims to leverage the expertise of the ethical hacker community to find vulnerabilities in Software and surrounding ecosystem to keep Customers' use of the Software safe from malicious activities.

3.13.3. UiPath shall perform annual penetration testing for Cloud Software systems and applications that process Customer Data, including after significant system and application changes. UiPath shall implement a patch and vulnerability management process to identify, report, and remediate application and system vulnerabilities that is approved by the application or system owner and is commensurate with the level of risk by (a) performing code and Cloud Software vulnerability scans on a regular basis and during any major system or application updates; (b) implementing provider patches or fixes; and (c) developing a risk treatment plan to address identified vulnerabilities.

4. INTERNAL SECURITY PRACTICES

4.1. Access Controls

4.1.1. UiPath employees are granted logical access to business resources that they have been specifically authorized to use in accordance with defined access control policies and processes. The access rights are granted as appropriate for employees to conduct their duties and adjusted upon a change in role and are removed upon termination of employment.

4.1.2. With respect to Cloud Software, UiPath reviews user access rights for appropriateness on a quarterly basis and shall immediately revoke inappropriate or unauthorized access upon detection.

4.1.3. UiPath employs a strong password policy, along with single sign-on on all enterprise applications and systems. For Customer end user authentication, UiPath shall use reasonable efforts to support authentication as described in applicable public user documentation: https://docs.uipath.com/automation-suite/docs/about-accounts (or successor website) and https://docs.uipath.com/automation-cloud/docs/about-accounts (or successor website). Users are required by policy to maintain the confidentiality of their passwords and change them periodically.

4.1.4. Users' logical access to Cloud Software is controlled and logged. UiPath has logging enabled for log-on activities on systems and generates alerts for unusual log-on behavior.

4.1.5. Owners of critical business systems and applications grant, review, and remove users' logical access to business systems, based on the principles of least privilege and segregation of duties.

4.1.6. With respect to privileged user accounts, UiPath use reasonable efforts to (a) restrict access to personnel with clear business needs; (b) provision accounts for the duration needed to complete the necessary task, (c) capture and periodically review system logs, and (d) enable access using multi-factor authentication.

4.2. Risk Management

4.2.1 UiPath has a risk management process in place. Risk assessments are conducted at least annually and identified risks are mitigated according to severity and business priorities. UiPath shall maintain an appropriate internal control system and operate an appropriate risk management system as further detailed under this Exhibit. UiPath commissions independent auditing companies to conduct annual audits of the design and operating effectiveness of controls and issue the respective documentation.

4.3. Physical Security

4.3.1. Physical security measures are designed to prevent unauthorized physical access or damage caused by physical and environmental threats to UiPath employees, premises, system and network devices and information, or interruptions to the organization's activities. The level of security measures, policies and

procedures implemented commensurate with the legal, regulatory, or contractual requirements associated with each facility.

4.3.2. Access to premises is monitored through access controls, such as individual badges and video surveillance, as permitted by the applicable law. Asset movement controls are in place, and the buildings are protected for seismic, flood and similar risks.

4.3.3. UiPath has a "no-paper" policy and, unless required by applicable law, aims to use electronic records and documents. UiPath has a clear desk and clear screen policy.

4.4. Asset Management

4.4.1. UiPath information assets are protected throughout the information lifecycle, including entry into UiPath systems, secure data transmission, and appropriate data access, storage, retention, and disposal. UiPath information assets are appropriately classified in terms of value, legal and contractual requirements to enable employees to handle them appropriately.

4.4.2. UiPath requires its employees and contractors to comply with a set of security measures when handling UiPath devices and information. Each UiPath asset holding confidential information has an identified asset owner and is kept in an inventory that covers the entire lifecycle from purchase to disposal. Employees are required to return all equipment upon termination of employment.

4.4.3. UiPath shall implement and document system procedures and baseline configurations and shall not include unsupported software or hardware.

4.5. Disposal and Destruction of Data and IT Equipment

4.5.1 UiPath has controls in place to mitigate the risk of improper and unsecure disposal and destruction of data, technology equipment and components owned by UiPath, including over-writing, or physically destroying removable media, erasing, or destroying mobile devices and securely erasing storage space allocated by cloud services, according to the cloud provider's methodology.

4.5.2 UiPath maintains policies restricting the storage of Customer Data locally on the employees' devices or on removable media.

4.6. Mobile Devices and Teleworking

4.6.1. UiPath maintains adequate policies on teleworking and the access of Customer Data from remote devices. Corporate devices with access to Customer Data are adequately protected. Users are allowed to use their personal devices to access UiPath business resources under a limited policy restricting and controlling users' responsibilities and access to Customer Data.

4.6.2. UiPath applies security measures on employee devices, including by:

a) requiring a multi-factor authentication access control mechanism to give full access to Customer Data.

b) applying security patches to applications and system software bearing Customer Data in line with provider recommendations.

c) authorizing business applications before having access to Customer Data.

4.7. Human Resources Security

4.7.1. UiPath may perform background checks prior to employment, solely as permitted under applicable law.

4.7.2. UiPath ensures that employees agree to terms and conditions concerning confidentiality and information security appropriate to the nature and extent of access they will have to the organization's assets and that go beyond the duration of the employment period.

4.7.3. Responsibilities regarding information security are communicated to UiPath employees and they are informed that disciplinary actions can be taken against them based on violations of policies and procedures.

4.8. Third-Party Provider Risk Management

4.8.1. UiPath maintains a provider risk management program through which it assesses and manages the risks assumed by the nature of relationships with providers that receive, store, process, or host UiPath data or have access to UiPath network and systems.

4.8.2. UiPath checks the security measures of its providers that have access to Customer Data has a policy to enter into agreements concerning data protection and ancillary security requirements seeking to ensure that levels of confidentiality and data security consistent with the ones set out in this Exhibit are implemented by such providers .

4.8.3. UiPath strives to maintain the right to perform audits to monitor the compliance of its providers with the agreed technical and organizational measures regarding data confidentiality and security.

5. SECURITY INCIDENTS MANAGEMENT AND BUSINESS CONTINUITY

5.1. UiPath is committed to comply with contractual and legal obligations for the protection of Customer Data. UiPath has designed processes to provide response to Security Incidents, without undue delay, to minimize risks and ensure availability of information systems.

5.2. To respond to Security Incidents effectively and in a timely manner, UiPath Security Incidents management teams are taking necessary actions to contain the threat, eradicate the source of the Security Incidents, and restore the affected systems, information, and data.

5.3. Security Incident responders track the Security Incidents root causes, the lessons learned in the Security Incidents management system and propose continuous improvements to system and data owners.

5.4. UiPath utilizes a decentralized office approach so employees, and contractors are not dependent on specific office locations to perform their duties. Data processing environments maintain redundancy to meet availability requirements. Systems are built with failovers within availability zones. Data availability and continuity of service is ensured by using reputable cloud service providers.

5.5. UiPath will implement and maintain a formally documented Security Incidents management policy that includes (a) a reporting mechanism for actual Security Incidents and events affecting the security of Customer Data, including the reporting of actual unauthorized or unlawful access, disclosure, loss, alteration and destruction of Customer Data (b) procedures for notification to relevant authorities as required by applicable law and Customer; and (c) procedures for forensic investigation of a Security Incident.

5.6. UiPath shall perform business continuity risk assessments to determine relevant risks, threats, likelihood of a service outage or Security Incident, impacts of a service outage or Security Incident, and required controls and procedures to secure Customer Data. Based on risk assessment results, UiPath shall document, implement, annually test and review business continuity and disaster recovery plans to validate the ability to timely restore availability and access to Customer Data in the event of a service outage or Security Incident ("**BCDR Plan**"). In its BCDR Plan, UiPath shall include (a) availability requirements for Customer, specifying critical systems; (b) UiPath internally agreed recovery point objective ("**RPO**") and recovery time objective ("**RTO**"); (c) clearly defined roles and responsibilities; (d) provisions for a geographically separate site subject to physical and environmental controls; and (e) backup and restoration procedures that include sanitation, disposal, or destruction of data stored at the alternate site.

5.7. Following each Disaster after Cloud Software have been fully restored, UiPath shall conduct a root cause analysis and provide to Customer a summary report that describes, at a minimum, (i) the causes of the Disaster, (ii) efforts taken to mitigate the consequences and resolve the Disaster, and (iii) the remedial actions to be implemented by UiPath in order to avoid future Disasters.

5.8. If UiPath becomes aware that a Security Incident has occurred, UiPath will, without undue delay: (1) notify Customer of the Security Incident, without compromise to UiPath's investigation or response; (2) investigate the Security Incident and provide Customer with reasonable information about the Security Incident; and (3) take reasonable steps to mitigate the effects resulting from the Security Incident. The notice shall be sent

to an e-mail address provided by Customer and available in UiPath's records. Customer is responsible for providing appropriate and updated contact information. The Parties agree that, by the mere act of giving notice of a Security Incident, UiPath does not acknowledge any liability or fault thereof. Customer acknowledges that it is responsible for complying with its own legal obligations regarding Security Incident notifications. If Customer suspects that a Security Incident occurred, Customer shall without undue delay notify UiPath at privacy@uipath.com.

6. AWARENESS AND TRAINING

6.1. UiPath maintains an annual internal training program to educate its employees with respect to UiPath information security and compliance-related policies. Employees are informed of the requirements for acceptable use of UiPath resources, in order to mitigate the risk of unauthorized access to UiPath equipment, as well as use and modification of information assets.

6.2. UiPath trains employees on information security upon hire and annually thereafter. UiPath updates the training to include changes in its organizational policies and procedures and addresses: (a) employees' specific job functions; (b) disciplinary actions when Personnel commit or cause a Security Incident, and (c) specific training for the processing of personal data in accordance with applicable data protection laws.

7. POLICY MONITORING, TESTING AND REVIEWING

7.1. UiPath reviews policies at least annually and updates as needed to ensure that policies comply with changes in law, common industry standards, organizational practices, and contractual obligations and that they are appropriate to the risks faced by UiPath.

8. CUSTOMER ASSESSMENT

8.1. UiPath shall promptly review and complete any justified Customer security questionnaire. UiPath shall make relevant documentation, reports, and evidence available for review upon Customer's written justified request.

9. AUDIT AND GOVERNMENT ACCESS

9.1. If Customer believes, acting reasonably and in good faith, that an on-site or remote audit is necessary to verify compliance with this Exhibit, Customer may request that it or a third party conducts an audit, which shall be subject to the conditions set out below.

a) an audit plan must be agreed by the Parties and, if applicable, the third party auditor, with eight (8) weeks in advance of the proposed audit date; the audit plan will describe the scope, duration (not to exceed thirty calendars days), third party auditor and start date of the audit and shall be limited as to ensure the UiPath's confidentiality and security obligations towards its employees and counterparties.

b) if the audit scope described in the audit plan is addressed in one of the Security Certifications and Attestations performed by a qualified third party in the twelve (12) months prior to Customer's audit request, and to the extent such Security Certifications and Attestations allow Customer to comply with its regulatory obligations, Customer agrees to accept and rely on these artifacts and UiPath's confirmation that there were no material changes in the verified data protection/security measures, and therefore no audit will be performed.

c) Customer may use an independent auditor to conduct the audit on its behalf, provided that Customer confirms with reasonable prior written notice that such auditor is authorized to act on behalf of Customer.

d) audits may be performed no more than once (1) a year (unless otherwise required by Applicable Law and/or Customer's regulators) and must be conducted during UiPath's business hours and will not interfere with UiPath's business activities. The audit will be conducted in a manner that avoids any unreasonable or unnecessary disruption to UiPath's operations.

e) The audit will be performed under the coordination and supervision of UiPath, in accordance with UiPath security-related policies and procedures to ensure the safety of the persons involved and to protect the

security and confidentiality of Customer Data.

f) UiPath will designate and make available to Customer a reasonable number of appropriately qualified and knowledgeable UiPath employees to facilitate the audit.

g) the scope of the audit must be limited to records/information, products and processes solely tied to the delivery of contracted Software.

h) audits may be performed only if a confidentiality agreement is concluded with the third-party auditor and the audit results will remain confidential and will not be shared with any third party unless agreed by an authorized legal representative of UiPath in writing.

i) unless prohibited by the applicable laws, Customer must provide UiPath with a copy of the audit report free of charge.

j) audits are performed at Customer's expense and payment will be made in accordance with the payment provisions in the Agreement.

k) UiPath will give reasonable cooperation and assistance.

9.2. If UiPath receives any valid request of disclosure of Customer Data from a governmental body, it will: (a) make all reasonable efforts to redirect the request to Customer; (b) notify Customer as soon as possible after receiving a request, unless prohibited by law to send such notification. In such case, UiPath will make all lawful efforts to waive such prohibition; (c) challenge the legality of such order to disclose if, after a careful assessment, it concludes that there are grounds under the law of the country of destination to do so. If UiPath is still compelled to disclose Customer Data, it will disclose only the minimum amount of data necessary to comply with the request of disclosure.

10. SECURITY TESTING

10.1. This Section applies where the Software is supporting critical or important functions of Customer. Exercise of such rights shall be subject to the principle of proportionality concerning whether the Software is used for critical or important functions of Customer's operations.

10.2. UiPath performs penetration testing of its Software. Such testing shall be performed by UiPath at least annually, by employing an independent third party. Upon written request of Customer, UiPath shall share a penetration testing summary report with Customer.

11. REPORTING AND MONITORING

11.1. Where Customer has a right to monitor UiPath's performance on a regular basis, Customer shall do so by having access to real-time monitoring of UiPath's Cloud Software performance, inclusive of the observance of the agreed service level agreement commitments, made accessible via status.uipath.com (or successor website). Customer may also elect to enroll in the UiPath premium support offerings, wherein a designated technical account manager may act as the primary liaison for the daily management of the services acquired by Customer and will also directly attend to the relationship between Customer and UiPath.

12. GOVERNANCE

12.1. UiPath reserves the right to make additional changes to this Exhibit and publish them on the Trust Portal, provided that UiPath will not decrease the level of security provided hereunder.

****