Information Security Exhibit

Data security sits at the foundation of product development at UiPath (hereinafter, "**UiPath**"). This Information Security Exhibit (the "**Exhibit**") points out the organizational policies and controls in effect at UiPath that are aimed towards maintaining confidentiality, integrity, and availability of Customer Data used with UiPath products or services (hereinafter, the "**Software**"). Unless defined herein, terms used with capital letters will have the meaning given to them in the applicable Agreement.

"Agreement" means the agreement validly executed between UiPath and the Customer with respect to access to, and use of, paid Software and/or Services, 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).

"Cloud Software" means Software as a service provided to the Customer.

"Customer" means the entity using paid Software and/or Services under an Agreement.

"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.

"Documentation" means the official public user documentation for Software as made available on the Trust Portal.

"On-Premise Software" means Software deployed on Customer premises.

"Personal Data" means (i) information related to an identified or identifiable natural person as defined by, as applicable, Regulation (EU) 2016/679 ("**GDPR**"), the California Consumer Privacy Act ("**CCPA**"), and other applicable privacy laws ("**PII**"), (ii) protected health information, as regulated by the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") ("**PHI**"), and (iii) cardholder data ("**CHD**") and/or sensitive authentication data ("**SAD**"), as defined by the Payment Card Industry Data Security Standard ("**PCI DSS**").

"Services" means professional services specified in an Order, excluding Support.

"Software" means software products developed by or for UiPath and/or its Affiliates and licensed to Customer as specified in accepted orders, which may be provided, as available as "**Cloud Software**" or "**On-Premise Software**", and excludes Third- Party Services.

"Support" means maintenance and service, applicable to the Software during the License Term as provided in the support terms available on the Trust Portal.

"Third-Party Services" means the cloud applications, cloud service endpoints, data services, software, application programing interfaces, and content of third parties which may be accessed using the Software or Services.

"UiPath Internal Policies" means the collection of policies maintained available by UiPath with respect to confidentiality, information security, and intellectual property protection.

1. SCOPE

1.1. This Exhibit highlights security measures maintained by UiPath with respect to its internal infrastructure and its Software, that could have an impact on 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 expressly 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 to vendors that have access to Customer Data can be found at: https://www.uipath.com/assets/downloads/cybersecurity-requirements.

2. SECURITY CERTIFICATIONS AND ATTESTATIONS

1.3. UiPath recognizes the importance of implementing appropriate technical and organizational security measures and adequate security controls to prevent any 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. Further information is available on the Trust Portal, or upon Customer request. A list of certifications and attestations is available below, and further information on the Software in scope is available on the Trust Portal, or upon Customer request:

a) ISO/IEC 27001 certification

b) SOC 2 Type 2 attestation

c) Cyber Essentials Plus (CE+) certification

1.4. UiPath is constantly working to improve its quality and security standards and is working on an internal roadmap of certifications 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.

1.5. UiPath shall also comply with the controls in, and maintain, an ISO/IEC 27001 certification, providing that certification and a copy of the corresponding statement of applicability ("**SOA**") to Customer upon written request.

2. PRODUCT SECURITY

2.1. Product Development Practices

2.1.1. UiPath follows a secure software development lifecycle ("**SDLC**") for developing products. The secure 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.

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

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

2.1.4. Additionally, UiPath shall restrict and track personnel access to program source code and require developers to periodically attend secure system development training.

2.2. Cryptographic Controls

2.2.1. 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, as detailed in the relevant Documentation.

2.2.2. Only industry-standard algorithms for encryption and key strength that are approved by UiPath engineering and IT departments are used to encrypt UiPath 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.

2.2.3. 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 they are protected from modification, loss, destruction, and unauthorized disclosure during their lifecycle (use, storage, and handling).

2.3. Network Security and Operations

2.3.1. All the web services offered as part of Software are enabled for TLS 1.2+.

2.3.2. Intrusion prevention and detection systems 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.

2.3.3. 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 and the organization's exposure to such vulnerabilities.

2.4. Software Access Controls

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

2.5. Access to Customer Data

2.5.1. UiPath does not have access to Customer Data used by the Customer with On-Premises Software unless access is expressly granted by the Customer.

2.5.2. UiPath personnel may have access to Customer Data used by the Customer with Cloud Software solely for the purpose of fulfilling UiPath rights and obligations under the Agreement. UiPath leverages privileged account management to minimize granting access of UiPath personnel to Customer Data in Cloud Software. UiPath personnel who need to edit system resources, access, or modify Customer Data must use privileged account management to temporarily raise their access level. Privileged account management requests must be enjoined by an adequate reason for access and are subject to approval by UiPath authorized reviewers. The activity conducted while using privileged account management is logged and recorded.

2.5.3. Unless otherwise agreed, UiPath shall restrict third party access to Customer Data.

2.6. Tenant Data Segregation

2.6.1. 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.

2.7. Customer Data Hosting

2.7.1. As part of the Software, UiPath may use third-party service providers which may have access to Customer Data, as sub- processors of UiPath.

UiPath maintains the list of sub-processors on the Trust Portal.

2.7.2. Customer Data and Personal Data uploaded by the Customer in the Software will be hosted in the region(s) evidenced in the Sub-processor list. Where technically implemented in a particular Software component, the Customer may configure the hosting location of the Customer Data used therein, provided however that back-ups may have different configurations.

2.8. **Customer Data Back-ups**

2.8.1. Regular back-ups 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.

2.8.2. 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.

2.9. **Customer Data Retention**

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

2.10. **Logs Information**

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

2.10.2. UiPath enables operational logs and security logs of activity in Cloud Software. Operational logs are used for monitoring uptime and availability of infrastructure and Cloud Software. Security logs are used for identifying security incidents, policy violations, fraudulent activity, auditing, and forensic analysis, supporting investigations, establishing baselines, and identifying trends and potential long-term problems.

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

2.11. **Personal Data Protection**

2.11.1. UiPath takes Personal Data protection very seriously and encourages Customers to minimize the use of Personal Data with Cloud Software, in line with the principles of the applicable legislation. Further rights and obligations between UiPath and Customer with respect to protection of Personal Data as part of Customer Data will be governed by appropriate data protection agreements executed between the Parties in accordance with GDPR and any applicable legislation.

2.11.2. Though UiPath is committed to making its operating environment as compliant as possible, 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, except where UiPath has expressly instructed otherwise in the Documentation, or by updates to this Exhibit or the Trust Portal. Nonetheless, the 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.

2.11.3. UiPath, in its capacity as data controller, makes available a process for data subject access requests, as required by the GDPR, available on the Trust Portal. UiPath will notify the Customer without undue delay of any data subject requests which UiPath in its capacity as data processor may receive but to which the Customer in its capacity as data controller must respond.

2.11.4. As a controller, UiPath processes Personal Data in accordance with its Privacy Policy available on the Trust Portal.

2.12. **Malware**

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

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

2.13. **Vulnerabilities Management**

2.13.1. 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.

2.13.2. Regular testing is also performed directly against 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.

2.13.3. 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 vendor patches or fixes; and (c) developing a risk treatment plan to address identified vulnerabilities.

3. INTERNAL SECURITY PRACTICES

3.1. Access Controls

3.1.1. 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.

3.1.2. Application owners shall review user access rights for appropriateness on a quarterly basis and shall immediately revoke inappropriate or unauthorized access upon detection.

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

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

3.1.5. 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.

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

3.2. Risk Management

3.2.1. UiPath has a risk management process in place designed to reduce the risks to an acceptable level. Risk assessments are conducted at least annually and identified risks are mitigated according to severity and business priorities.

3.3. Physical Security

3.3.1. 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.

3.3.2. 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.

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

3.4. Asset Management

3.4.1. 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.

3.4.2. 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.

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

3.5. Disposal and Destruction of Data and IT Equipment

3.5.1. 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.

3.5.2. UiPath maintains policies in place restricting the storage of Customer Data locally, on the employees' devices or on removable media.

3.6. Mobile Devices and Teleworking

3.6.1. 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.

3.6.2. 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 vendor recommendations.

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

3.7. **Human Resources Security**

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

3.7.2. 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.

3.7.3. 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.

3.8. **Vendor Risk Management**

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

3.8.2. UiPath checks the security measures of its critical vendors and has a policy to enter into data protection agreements seeking to ensure that at least the same level of confidentiality and data security is implemented by its sub-contractors as the ones applicable to UiPath.

3.8.3. UiPath strives to maintain the right to perform audits to monitor the compliance of its sub-contractors with the agreed technical and organizational measures regarding data confidentiality and security.

4. INCIDENT MANAGEMENT AND BUSINESS CONTINUITY

4.1. 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 and operational incidents, with undue delay, to minimize risks and ensure availability of information systems.

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

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

4.4. UiPath utilizes a decentralized office approach and 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.

4.5. UiPath shall implement and maintain a formally documented incident management policy that includes (a) a reporting mechanism for actual 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 the Customer; and (c) procedures for forensic investigation of a security incident.

4.6. UiPath and its sub-processors shall implement, install and maintain the following environmental controls to protect personnel and equipment used to process or store Customer Data: (a) fire suppression systems; (b) temperature and humidity controls within a data center or server room environment; (c) arrangements with authorities for active response to civil unrest or natural disasters; and (d) backup power technology (e.g., uninterruptible power supply, diesel generator, separate grid connection, etc.).

4.7. UiPath shall perform an environmental risk assessment before processing any Customer Data, which shall include an assessment of the threats of natural and man-made disasters. UiPath shall implement appropriate physical protections for facilities storing Customer Data, taking into account the results of the environmental Risk Assessment, the availability of state- of-the-art technology, and the costs of implementing those measures.

4.8. UiPath shall perform business continuity risk assessments to determine relevant risks, threats, likelihood of a service outage or security breach, impacts of a service outage or security breach, 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 data breach ("**BCDR Plan**"). In its BCDR Plan, UiPath shall include (a) availability requirements for the 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.

4.9. Following each Disaster after the 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 cause or 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. AWARENESS AND TRAINING

5.1. 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 mitigate the risk of unauthorized access to UiPath equipment, as well as use and modification of information assets.

5.2. UiPath shall train employees on information security upon hire and annually thereafter. UiPath shall update that training to include changes in its organizational policies and procedures and shall address (a) employees' specific job functions; (b) disciplinary actions when Personnel commit or cause a suspected or actual Data Breach, and (c) specific training for the processing of personal data in accordance with applicable Data Protection Laws.

6. POLICY MONITORING, TESTING AND REVIEWING

6.1. 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.

7. CUSTOMER ASSESSMENT

7.1. 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.

7.2. Without the need for confidentiality measures, Customer may share the results of any audit, report, or test under this Section 8 with any Affiliate or any government regulator of any Affiliate. Under appropriate confidentiality measures, Customer may share the results of any audit, report, or test under this Section 8 with actual or prospective clients of any Affiliate. To the extent required, UiPath shall cooperate in good faith with requests from any client or government regulator of any Affiliate that wishes to further investigate UiPath security audit attestations and results.

8. GOVERNANCE

8.1. 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.

****