UiPath Procurement Cybersecurity Requirements

The technical and organizational measures provided below apply to all the services ("**Services**") and/or products ("**Products**") provided by the Vendor in the framework of the applicable Agreement. Nothing in this document may be construed or interpreted as being contrary to the provisions of the Data Processing Agreement ("**DPA**"), if such DPA is concluded between UiPath and the Vendor (as defined by the applicable Agreement).

1. Security Policies and Governance

Vendor's information security capabilities are supported by documented IT security policies and practices that are mandatory for all Vendor employees and managed through an information security governance framework. The policies define clear information protection roles, responsibilities, and accountability, and include appropriate administrative, logical, technical, and physical safeguards that comply with this document. Vendor will update and/or review such policies, as necessary, on no less than an annual basis or upon a material change in the provision of Services. Vendor will ensure that the policies comply with applicable law and industry standards (e.g., ISO/IEC 27001 and 27002; US National Institute of Standards and Technology [NIST] Cybersecurity Framework, and US NIST 800-53).

2. Security Incidents

Vendor will maintain a security incident response plan and follow documented security incident response procedures including data breach notification to UiPath without undue delay where a data breach is known or reasonably suspected to affect UiPath data, systems, or the provision of Services to UiPath. In the case of a breach of security, Vendor will promptly at its expense investigate such breach, mitigate the effects of the breach and perform post-incident assessment(s), including those reasonably requested by UiPath, and report on the results of such assessment(s) to UiPath.

Vendor will promptly provide UiPath with, at a minimum, information to assist UiPath in its own reporting obligations relating to the breach. In the event of any disclosure or loss of, or inability to account for any UiPath data, Vendor will be solely responsible for the costs of remedying any data incident caused by a breach or by the Vendor of its obligations under the applicable Agreement, including the cost to provide any notices and credit services required by applicable law to third parties, and all associated support to such third parties.

Vendor must immediately report security events potentially or actually involving UiPath systems or data to security.breach@uipath.com. At a minimum, the report should include the date and time of the event, a description of the event, who observed the event, equipment involved and type of data involved.

3. Data Handling

Vendor will maintain an inventory of UiPath data in Vendor's possession, including disposal instructions upon contract closure. Computing environments with resources containing UiPath data will be logged and monitored. Vendor will assess risks related to processing of UiPath data in Vendor's possession and create an action plan to mitigate identified risks.

4. Human Resources

Vendor must have comprehensive human resources (HR) processes and a security awareness program for all personnel that will access facilities, networks, environments and/or confidential information or have custody of UiPath products, assets or data. Vendor employees will complete security and privacy education annually and certify each year that they will comply with ethical business conduct, confidentiality, and security policies. Records of annual training completion must be documented and retained for tracking purposes.

Vendor must perform background checks, consistent with local law, for all personnel with access to UiPath facilities, networks, environments, and/or confidential or proprietary business information prior to permitting such access.

In the event Vendor personnel no longer perform tasks on behalf of UiPath, Vendor must promptly ensure that access to UiPath facilities, networks, environments and/or confidential or proprietary business information is terminated, and all associated accounts removed.

Vendor is authorized to use subcontractors for the provision of the services as long as those subcontractors are contractually bound to comply with security standards consistent with those set forth in this document. Vendor will maintain a list specifying its subcontractors, the country of destination of the data, and will provide that list to UiPath upon reasonable notice. UiPath may, reject the use of any subcontractor for justified reasons and as described in Section 8 to the DPA.

Vendors who are found to violate the code of business conduct or other Vendor policies related to privacy and security may be subject to action including litigation or termination of contract.

5. User Access Management

Vendor will maintain proper controls for requesting, approving, granting, modifying, revoking, and revalidating user access to systems and applications containing UiPath data. All access requests will be approved based on individual role-based access control and reviewed on a regular basis for continued business need.

All systems must meet corporate IT security standards and employ security configurations and security hygiene practices to protect against unauthorized access to operating system resources. Vendor will limit privileged access to authorized individuals for a limited period of time and usage, which will be

monitored, logged, revalidated regularly and discontinued when no longer needed. Any shared access will be for a limited period of time and usage, which will be monitored. logged, revalidated regularly and discontinued when no longer needed.

Production environments are logically segregated from non-production environments. Installation of software or programs in the production environment requires approval by appropriate personnel. Vendor will keep UiPath data segmented from other companies' data.

6. Personal Equipment

Vendor must ensure that personal equipment of Vendor personnel is not used to store, access or process UiPath data and/or information.

7. Authentication

Vendor will create unique identifiers for Vendor user accounts and prevent the reuse of identifiers. Account login parameters follow these rules:

- accounts are not shared.
- inactive sessions are password protected after a period of inactivity.
- accounts are locked after a number of failed login attempts.
- user and device authentication to information systems is protected by passwords that meet password complexity requirements.

8. Password

When granted access to UiPath systems, Vendor must comply with UiPath password parameters and access control requirements.

9. Encryption

Vendor will encrypt UiPath data when storing, receiving, transmitting and/or communicating it across the Internet, on a wireless network, or otherwise outside of Vendor's secure premises, with an industry-recognized encryption system. Passwords stored in databases must be one way hashed or encrypted. Prior to being backed-up, UiPath data will be encrypted or equivalently secured.

10. Physical Security

Vendor will implement the physical security of its own facilities including data centers as well as take precautions against environmental threats and power disruptions for facilities used to process UiPath data or provide services to UiPath. Physical security controls include appropriate alarm systems, access controls (including off-hours controls), visitor access procedures, security guard force, fire suppression, video surveillance as deemed necessary. Access to the data center and controlled areas within the data center will be limited by job role and subject to authorized approval.

11. System and Network Security

Vendor will employ encrypted and authenticated remote connectivity to Vendor computing environments and UiPath's system unless otherwise directed by UiPath. Vendor will implement technical and organizational measures to support network security as well as the availability of computing environments including access to UiPath data. Network security measures include, but are not limited to, firewalls; remote access control via virtual private networks or remote access solutions; network segmentation, and detection of unauthorized or malicious network activity via security logging and monitoring. Vendor will perform routine scans for vulnerabilities, intrusions and unauthorized changes and install host-intrusion prevention system on all servers, if applicable.

12. Server Configuration Security

Measures will be taken to ensure server configuration security, including but not limited to:

- Operating systems will be hardened and documented.
- Unused services, applications and ports will be disabled where possible.
- Access to services must be logged and protected by access control methods and in accordance with access control policies.
- The latest patches of security must be installed on systems following successful testing.
- Trust relationships must be avoided between servers. The "least privilege" security principle will be used to perform a function.
- Appropriate measures should be taken to deal with denial of service (DOS) and distributed denial of service (DDOS) attacks.

13. Business Continuity and Disaster Recovery

Vendor will have defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Backup data intended for off-site storage will be encrypted prior to transport.

14. Media Handling

Vendor will implement protections to secure portable storage media from damage, destruction, theft, or unauthorized copying and the UiPath data stored on portable media through encryption and secure removal of data when no longer needed. Additional similar measures will be implemented for mobile computing devices to protect UiPath data.

15. Workstation Protection

Vendor will implement protections on end-user devices and monitor those devices to be in compliance with the security standard requiring hard drive passwords, screen savers, antivirus software, firewall software, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate workstation compliance deviations. All email traffic will be scanned for malware. Vendor will implement policies and/or technical controls that prohibit the transfer of UiPath data by portable storage mediums or email unless strictly necessary, and then only to an encrypted portable storage medium or by encrypted email. Additionally, full disk or device encryption is required for all portable storage mediums and media that store UiPath data. Vendor will securely sanitize physical media intended for reuse prior to such reuse and will destroy physical media not intended for reuse.

16. Cloud Services

If the Services provided in the applicable Agreement are cloud-based, Vendor will maintain (a) critical information system logs (e.g., a security information and event management [SIEM] solution to aggregate and correlate logged events). In order to protect against unauthorized access and modification, Vendor ensures that network logs, operating system logs, application logs and intrusion detections events are captured. Application user activity will also be logged by the application, (b) security monitoring and evaluation. Vendor will define security monitoring alert criteria, how alert criteria will be flagged, and will identify authorized personnel for flagged system alerts. Vendor will define availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.

17. Service and Product Security

Vendor will ensure source code is checked for vulnerabilities using code analysis tools prior to being released into production. Vendor, including its subcontractors, shall take all commercially reasonable measures, such as but not limited to up-to- date virus detection and the timely installment of security patches, in order to guarantee that every Product and/or Service provided by him to UiPath or used on UiPath's network shall be free of viruses, malware or any malicious code in general that could hinder or adversely affect the functioning of the computers, the network, the access to or the use of computer programs or that affects UiPath's data. Vendor will keep documentation of third-party libraries being used in its service and monitor vulnerabilities in dependencies. Vendor will restrict access to program source code.

18. Threat and Vulnerability Management

Vendor will maintain measures meant to identify, manage, mitigate and/or remediate vulnerabilities within the Vendor computing environments. Security measures include:

- patch management
- anti-virus / anti-malware
- threat notification advisories
- vulnerability scanning (all internal systems) and periodic penetration testing (internet facing systems) within remediation of identified vulnerabilities.

At least annually, Vendor will engage with a third party to perform penetration testing, assign risk ratings to discovered vulnerabilities, and track vulnerabilities through resolution.

19. Third Party Management

On a periodic basis, Vendor management reviews controls within third-party assurance reports to ensure that they meet organizational requirements. If control gaps are identified in the assurance reports, management addresses the impact that disclosed gaps have on the organization. Vendor performs a risk assessment to determine the data types that can be shared with a managed service provider. Vendor will disclose to UiPath the use of any shared third-party hosting facilities that will hold UiPath data, and it will take reasonable measures to ensure such third parties materially comply with the applicable terms of this document.

20. Right to Monitor

UiPath reserves the right to monitor access and use of its data and systems to prevent improper or unauthorized use and to ensure compliance with the UiPath security requirements. However, in any event (i) UiPath will only undertake such monitoring with the Vendor's authorization (which shall not be unreasonably withheld) and (ii) such monitoring will not materially disrupt or impair the operations of the Vendor's systems.

21. Audit

Vendor will respond to reasonable information requests, for example by completing Standardized Information Gathering (SIG) questionnaires or similar information security questionnaires on a regular basis. UiPath may exercise its right of audit under EU data protection laws. Vendor will provide to UiPath, its auditors (including internal audit staff and external auditors), inspectors, regulators, and other representatives as UiPath may designate in writing, access to any of its owned or managed facility at which the Vendor is providing the Services, to relevant employees, and to data and records relating to the Services for the purpose of performing audits and inspections to verify compliance with the Security Requirements. Vendor will also provide audit reports or certifications not older than twelve (12) months by independent external auditors demonstrating that Vendor's technical and organizational measures are in accordance with industry standards (e.g., ISO/IEC 27001 and 27018 standards).