INFORMATION SECURITY AND PRIVACY REQUIREMENTS

Scope	**These Information Security Requirements apply to all UiPath Vendors which access, operate, process, store or otherwise manipulate UiPath Information which means any and all information made available by UiPath to Vendor during the business relationship, which may include, but not be limited to, confidential information (including but not limited to any document and information to which the Vendor has access during the performance of the business relationship, technical information, business methods, software programs, licensing model), personal data and any other proprietary information of UiPath. This way, UiPath strives to ensure that an appropriate level of information security is maintained at all times in its supply chain.**
Security Policies	Vendor ensures formal management commitment and efficient user awareness, by developing and distributing a comprehensive, approved information security policy and user guidelines to all individuals with access to Vendor's information and systems.
Organization of Security	Vendor designates members of its personnel with overall accountability for security and risk issues and provide appropriate authority and means to this function to co-ordinate the activity across the organization. Vendor segregates duties and areas of responsibility in the areas of security to reduce the risk of accidental or deliberate system or application misuse. Vendor's designated personnel shall be aware of all applicable statutory and contractual requirements, including but not limited to those in this document and export compliance, affecting Vendor's security controls, processes and systems.
Human Resources Security	Vendor ensures that all members of Vendor's personnel in charge with UiPath's Information: (i) are qualified and adequately trained in respect of security matters; (ii) are subject to systematic staff vetting processes for checking identity and background; (iii) are made aware of the confidential nature of UiPath Information and of the requirements in this document.
Asset Management	Vendor shall maintain an up to date list of the authorized information and technologies equipment that is used to access, transfer, process and/or store UiPath Information. Upon request, Vendor shall provide UiPath with a list of all the systems and devices where UiPath Information is stored or processed (*e.g.,* physical location, network location and business purpose of storing/processing). Vendor shall not store UiPath information on mobile devices (PDA's, laptops, USB drives, etc.) unless encrypted by state-of-the-art products/ standards. Any used or broken storage media containing UiPath Information shall be effectively wiped or destroyed prior to being decommissioned or reused.
Access Security	Vendor establishes and enforces written procedures to control the access to systems and services that may contain UiPath Information. Vendor identifies and records the connections with UiPath networks and systems. Vendor maintains an up to date list of user authorizations on its systems, allocates unique personal user IDs and all access to UiPath Information is controlled by strong passwords. Vendor ensures the user request and authorization process for access rights to its own systems and to UiPath systems is traceable. Vendor ensures that all system and network accesses are logged and maintained for a reasonable duration, but no less than 1 year. Vendor ensures that the systems on which UiPath Information is stored or processed, or from which UiPath systems are accessed, are protected against unauthorized accesses, unauthorized or accidental acquisition, destruction, loss, alteration or use. Vendor isolates UiPath Information from its own information and other customers' information so that only authorized staff can access UiPath Information.
Physical and Environmental Security	Access to Vendor's buildings, offices and computing facilities is controlled and limited (e.g. by use of locked doors, swipe card readers, burglary prevention, detection and response) in order to efficiently protect the confidentiality of information and access to critical systems, and to prevent theft of documents or equipment. Business-critical equipment is installed in a location where environmental risks are reduced, and appropriate environmental controls are deployed to mitigate any potential physical damage and is housed in secure areas and protected by perimeter security.
Operation Security	Vendor shall use all care and means available, including any state of the art technology, data loss mechanisms and anti-intrusion and/or anti-virus mechanisms, regularly updated on all devices, in order to prevent intrusion of malicious codes on all servers, workstations and all possible infrastructure (*e.g.* e-mail gateways, etc.), data corruption, data loss, loss of service. Should UiPath Information be transferred through data networks which are not under the direct control of the Vendor, Vendor takes all adequate actions to ensure both the confidentiality and the integrity of the data in transit. Data traffic from and to the Internet or other untrusted networks is limited using robust security mechanisms and monitored for abnormal behaviour, *e.g.* using proxies and gateways.
Third Party Access	Vendor ensures that no access is granted to UiPath Information without obtaining UiPath's prior written approval and shall cascade all these requirements to the lower tier supplier and/or subcontractor by means of a specific agreement made available to UiPath, upon request.

Information Security Incident Management	Vendor performs continuous monitoring of systems and networks, employs intrusion detection and prevention systems and records security events. Vendor implements a comprehensive and approved incident management process for information and systems that includes identification, response, recovery and post- implementation review of information security incidents. Vendor identifies and resolves incidents, minimizes their business impacts and reduces the risk of similar incidents occurrence. Should security incidents occur that affect UiPath systems or Information, Vendor shall immediately (and no later than 24 hours) report the incident to UiPath even without request and shall take any action to remedy detected or notified security incidents, including any actions that might be requested by UiPath. Vendor must provide a written report that comprises at least the following: (i) UiPath Information or systems affected by the security breach; (ii) actual or potential consequences of the security breach; and (iii) measures taken to mitigate and remove the effects of such breach.
Business Continuity Management	Vendor has a Business Continuity Plan for maintaining/restoring the services, information and equipment in the event of a major failure or of any kind of force majeure (including but not limited to: physical damage, power cuts, fire, natural disaster). Vendor has appropriate mechanisms, processes, defined roles and responsibilities in place to ensure on- going business processes and avoid major disruptions. Vendor documents and trains its employees on its business continuity plans to ensure that the business continues to function at an effective level in the event of a major incident. Such business continuity plans need to be regularly reviewed and tested.
Audit	UiPath may audit security of Vendor's systems, processes and procedures where UiPath Information may be stored or accessed. UiPath reserves the right, upon reasonable notice, to perform compliance and/or implementation audits. In the case of a significant change in Vendor's situation (including but not limited to mergers, acquisitions or other corporate re-organizations) or in its business activities, UiPath reserves the right to reassess the Vendor's compliance with UiPath security requirements as necessary to protect information and systems.
Privacy	Where access to Personal Data is required for the provision of services, Vendor will process such Personal Data in accordance with all applicable laws, including, the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "Regulation"). Where Vendor acts as data processor, it will comply with the obligations on data processors set forth by the Regulation, including: (i) process the Personal Data only in accordance with documented instructions from UiPath, including with regard to transfers of Personal Data to a country outside the European Economic Area; (ii) immediately inform UiPath if, in its opinion an instruction infringes the Regulation or there are any issues in complying with UiPath's instructions or implementing the required security measure to protect UiPath Personal Data; (iii) assist UiPath by appropriate technical and organizational measures for the fulfilment of UiPath obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the Regulation and, at the request of UiPath, assist in carrying out a data protection impact assessment prior to the processing of UiPath Personal Data; (iv) notify UiPath without undue delay after becoming aware of a Personal Data breach (meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, UiPath Personal Data transmitted, stored or otherwise processed), keep UiPath informed of any related developments and take all measures required, including assisting UiPath in notifying the breach to a supervisory authority and/or the data subjects concerned; (v) at the direction of UiPath, delete or return all UiPath Personal Data to UiPath after the end of the business relationship, and delete existing copies unless applicable law requires storage of the UiPath Personal Data; (vi) make available to UiPath all information necessary to demonstrate data protection compliance.
Termination	At, or before the start of the business relationship, Vendor shall provide UiPath with a termination plan that addresses how UiPath Information will be returned to UiPath, including backup and archival information, and how all UiPath Information will be permanently removed from Vendor's equipment and facilities.