INFORMATION SECURITY PRACTICES

Introduction	UiPath_is a global company committed to ensure the protection of confidential information & personal data. UiPath recognizes the importance of implementing appropriate technical and organizational security measures in order to prevent any unauthorized access, disclosure, alteration or destruction of such data. For this purpose, UiPath implements industry standard security controls. This is not meant to be the UiPath Security Policy but only a summary of the measures implemented for specific business activities. UiPath security measures follow a risk assessment approach and embrace the principles privacy and security by design.
Certifications and standards	Information security management - ISO 27001:2013 Quality management ISO 9001:2008 Respecting OWASP Secure Coding Practices VERACODE security assessments Legal compliance with the General Data Protection Regulation
UiPath relevant corporate security policies and procedures	Information Security policy Business continuity Plan Incident management process Security breach notification process
Human Resources Security	All UiPath employees are bound by confidentiality duties and have received awareness trainings regarding UiPath policies, including trainings on security and protection of personal data. Upon termination of a work relationship all access to information environments is removed and com company assets are retrieved.
Sub-contractors	UiPath has concluded data protection agreements with its vendors in order to ensure that at least the same level of confidentiality and data security is implemented by its sub-contractors. UiPath has the right to perform audits in order to monitor the compliance of its sub-contractors with the agreed technical and organizational measures regarding data confidentiality and security. Please check here the list of UiPath sub-processors: https://www.uipath.com/hubfs/Valentin/misc/Legal/UiPath%20Subprocessors.pdf

Physical and Environmental Security	Access to premises and production environment is monitored through access controls and video surveillance in the production environment, so that only authorized personnel has access to equipment and information. Asset movement controls are in place and the building is engineered for seismic, flood and other similar risks. In order to ensure data availability and integrity, cloud services are used for hosting data. All applications and infrastructure used in production are monitored.
Technical and access controls	Access to all systems is password protected and granted only to authorized personnel Two factor authentication and time-out of system access, as well as password complexity prevent inappropriate access. UiPath uses encryption for data in transit and at rest. Access of system administrators and operators are audited and critical security updates released are installed. Detection systems are in place to protect network security.