ptc

DIGITAL TRANSFORMS PHYSICAL

codebeamer™

Information Security Policy

Parametric Technology GmbH (PTC) is keenly aware of the importance of good information security management practices for both its business operations and for the utmost satisfaction of its customers.

Therefore, the company has decided to implement and continuously improve an Information Security Management System (ISMS) which conforms with the requirements of the ISO 27001 standard.

The ISMS's main objectives are:

- **to ensure full protection of data and information managed by PTC from fraudulent access,**
- **to assess the information security-related risks of our software applications and services as a highpriority issue,**
- **to give explicit guidance for all employees and contractors regarding information security implementation,**
- **to ensure a high standard of application security for PTC's own products.**

PTC is fully committed to living up to its customers' expectations to avoid and block cybersecurity attacks and reduce the risks of data loss and system disruption. In order to achieve those goals, PTC has defined security policies and implemented controls in the following areas:

Personnel Security

PTC has defined rules for the selection of its employees and for providing regular training on security measurements. The company has internal controls for the takeover process when employees are onboarded or leaving the organization, and internal checks in place regarding obligations originating from contracts with employees and contractors. These controls specifically cover the restriction of systems access and end-point security on different devices. Intland expects that all employees and long-term contractors are aware of and follow the rules of ethical behaviour.

Security of Environment

PTC strives to ensure that the internal and external infrastructure it relies on guarantees the safety and security of data and those of the services that PTC provides to their customers. With regards to services that involve the operation of external data centers, PTC resolves to only contract providers that adhere to the expected quality and security standards.

Application Security

PTC is committed to ensuring that its solutions comply with the most stringent security requirements. To achieve that goal, the company asserts its commitment to defining and maintaining a secure Software Development Lifecycle. Critical security incidents are handled with priority at all times. The company applies all the adequate best practices and tools that support its commitment to application security.

Supplier Conformance

In order to ensure that its services to customers meet the highest standards, Intland enlists the services of 3rd party providers. IT security concerns are taken into consideration and adequate assessments are carried out when selecting these providers. In order to minimize risks, PTC aims to contract with marketleading providers that have high numbers of satisfied customers.

Business Continuity and Disaster Recovery

Business continuity is a priority for Intland's executives, owners, and employees in order to ensure high-quality services to its customers. The company is in possession of reserve resources and specific processes that may be put into service to recover operations in the event of unexpected or high-risk situations. Regular exercises to assume business continuity and to resume operations are conducted with the declared frequency.

Intellectual Property Rights (IPR) and Personal Data Protection

The companies have measures in place to ensure maximal protection of the IPR of PTC products. End-user license agreements (EULA) and other documents governing the use of licenses are established and are revised on a regular basis. Intland is committed to protecting personal data and to complying with relevant legal statutes, and develops its own products accordingly. The company has established a GDPR policy and a Data Breach Action Plan.

PTC declares their commitment to planning and implementing actions to improve security in all the above areas and to executing regular monitoring and controlling activities in order to discover non-conformities and to take immediate corrective and preventive action for the continuous improvement of ISMS.

This Information Security Policy is:

- **Available, published and maintained as documented information**
- **Communicated, understood and applied within the organization**
- **Available to all relevant interested parties**
- **Periodically reviewed for ensuring its validity and suitability**

DIGITAL TRANSFORMS PHYSICAL