ptc

DIGITAL TRANSFORMS PHYSICAL

PTC Cybersecurity White Paper

WHITE PAPER

Contents

3 **PTC Security and Governance Framework**
Corporate Security Approach
Governance

5 **People**
Physical Security
Commitment to Competence
Employee Commitments
Cybersecurity & Privacy Training and Awareness

6 **Process**
Risk Assessment
- Internal Auditing
- Third-Party Vendor Risk Management

Incident Response

9 **Technology**
IT Technical Controls
- Network and Endpoint Security
- Device Security
- PTC User Account Security

PTC Products and Services
- Secure Software Development Lifecycle (SDLC) Program

PTC SaaS and Hosted Solutions
Technical Support

13 **Business Continuity**
Business Continuity Program

13 **Privacy**
Compliance with International Data Privacy Legislation
International Transfers of Personal Information
Product Data Collection

Purpose and Scope

The purpose of this document is to provide a summary of PTC's Security, Quality, Business Continuity, and Privacy programs to companies who are interested in conducting business with PTC. For more information, please contact your PTC Sales Representative or visit ptc.com/contact-us.

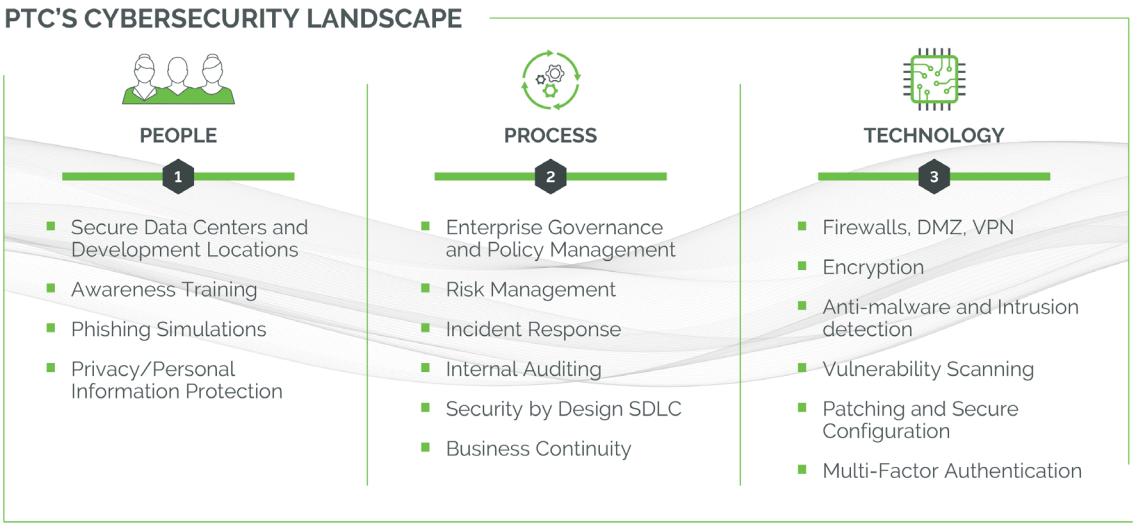
PTC Security and Governance Framework

Corporate Security Approach

PTC takes a holistic, multi-layered approach to Cybersecurity and Privacy that combines traditional Defense-in-Depth methods with next-generation Zero Trust principles. In today's globally interconnected world, every entry point on the attack surface must be considered critical. PTC is committed to securing the points under its control and appreciates the partnership of its suppliers and customers who diligently perform their obligations to apply updates, protect devices, and keep credentials secure.

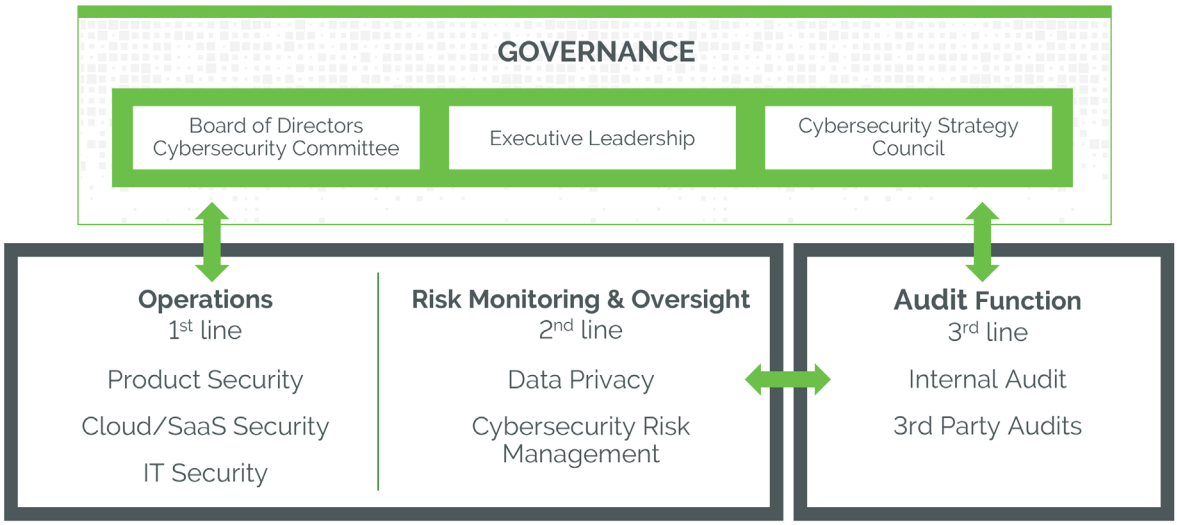
- People: PTC recognizes that technology alone cannot mitigate all security threats, and so we focus on developing our most critical resource: our people. Security is the responsibility of every PTC employee, contractor, or intern and is independent of departmental affiliation. PTC's corporate cybersecurity awareness activities are combined with role-specific tools and training to ensure that everyone has the knowledge and resources to meet their commitment to keep PTC safe.
- Process: An educated workforce then needs a governance framework to guide and monitor its activities. PTC has robust processes and policies in place to anticipate security risks and facilitate compliance with applicable regulations and standards, as well as address any incidents or violations. PTC focuses on continuous improvement and is constantly maturing its processes to keep pace with the rapidly evolving cybersecurity threat landscape.
- Technology: PTC seeks to automate these processes and remove the potential for human error whenever feasible by implementing technology solutions. From fundamental IT Security to development of our software products and keeping our customers' data safe in the cloud, PTC is dedicated to maintaining a secure infrastructure that is continuously monitored for possible threats.

These three key elements of People, Process, and Technology are tightly interwoven to secure our environments and data.



Governance

Cybersecurity is a risk area with oversight at the highest levels of the organization, including the Executive Level, with a "Three Lines Model" to effectively address Cybersecurity, Risk Management and Control as depicted below. The overall operational program is led by a cross functional Cybersecurity Strategy Council. All Cybersecurity, Risk and Internal Audit functions report to the PTC Executive Leadership Team and PTC Board of Directors Cybersecurity Committee.



The Three Lines model is defined as follows:

- **Operations (1st line):** The Operational Management of an organization is responsible for implementing the security protections, managing the day-to-day risks, and ensuring that the application of policies is supported by appropriate procedures.
- **Risk Monitoring & Oversight (2nd line):** The 2nd line oversees the controls implemented by the 1st line. Performs routine monitoring of the risk, ensuring that controls are properly designed and operating effectively.
- **Audit Function (3rd line):** The 3rd line is an Audit Function that is independent of the influence of Operational Management and Risk Monitoring & Oversight Lines and has the responsibility of overseeing the functions of both the 1st Line and the 2nd Line. PTC's Internal Audit Team is supplemented by external auditors.

People

Physical Security

PTC operates in controlled-access facilities and has established an Enterprise Physical Security Policy. Depending on the facility, physical security controls include photo ID badges, entrance logging, video monitoring, detection systems and guest registration. Some of these controls are in place only in relevant areas such as data centers and systems holding sensitive data or other data and systems determined to need higher levels of physical protection. Where PTC is not the building owner, physical security for the building perimeter, including elevators and stairwells, is monitored by the building landlord.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. PTC assigns job responsibilities to personnel based on knowledge and skills needed to adequately perform each job. PTC reinforces these responsibilities by providing hands-on training during the initial period of employment, and continual hands-on training for new business processes or job responsibilities. All employees undergo an annual Performance Evaluation process.

Employee Commitments

All personnel, including PTC employees and contractors, who may have access to any confidential information (including customer data) and PTC's IT Systems, are contractually committed to protecting and preserving the confidentiality and integrity of such information and systems under their terms of employment or by signing an NDA.

PTC has both an Acceptable Use Policy (AUP), and an IT Security Policy that apply to all employees and contractors. To ensure that these user-based policies are supported by all employees, all new employees must provide a signed acknowledgment indicating that they have read, understand, and agree to abide by the rules of behavior in the Acceptable Use Policy before being authorized access to confidential information and PTC's IT systems. Annually, each employee must re-attest to having read and accepted the policy.

The AUP applies to all personnel, all facilities including home offices, third-party vendors, all PTC IT systems, and all PTC-required or maintained configurations or other elements of systems on external accounts where PTC software is being provided as SaaS. Among other controls, PTC's AUP requires that employees adhere to Clean Desk and Clear Screen procedures. VPN Connection is required for external access to internal PTC systems and requires two factors of authentication.
The policy includes a disciplinary process for policy violations. PTC's IT Security organization carries out periodic security scans of all PTC IT Systems to ensure compliance.

Cybersecurity & Privacy Training and Awareness

PTC's IT Security Department is responsible for ensuring all PTC Employees receive regular cybersecurity training and awareness. PTC's Cybersecurity Training and Awareness Program, which is incorporated in its IT Security Policy, includes:

- A Statement of Management's commitment to cybersecurity and privacy throughout PTC
- Requirement for all Employees to become familiar with and comply with PTC's IT Security Policies
- A Statement of personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to PTC, its employees, its customers, and third parties
- Contact points and resources for additional information and advice on cybersecurity matters
- Methods commonly used in intrusions that can be blocked through individual action
- A requirement that the training shall be regularly updated based on changes that occur in PTC's organizational structure, procedures, or technology that may impact cybersecurity requirements. If IT Security identifies such a need during the annual enterprise risk assessment or after a cybersecurity Incident, IT Security will supplement training with emails, posters, or activities.

PTC's Cybersecurity Training Program consists of the following training activities:

- PTC IT Security has rolled out advanced, role-based security training to a large group of PTC Employees. The role determines the training and number of hours required for the staff member.
- PTC Privacy Department requires all employees to take a Privacy & Information Security training that includes data handling and some cybersecurity topics such as: use of third-party storage sites, careful use of social media, and information security threats.
- PTC Compliance requires all employees to take an annual Code of Conduct training that includes cybersecurity topics such as: malware, phishing, trojans, social media.
- Lastly PTC has a cybersecurity awareness program that covers incremental topics based on current events.

Process

PTC's Cybersecurity Program is supported by robust processes and procedures at all levels. Our matrixed cybersecurity organization is governed by industry-standard frameworks, and to ensure that they are executed, we involve an executive leadership committee, a cross-functional Cybersecurity Strategy Council, business unit security leads and cybersecurity analysts across the enterprise. Quarterly updates on cybersecurity strategic plans, programs and initiatives are presented to the Board of Directors. Ongoing program assessments are performed to monitor progress and identify opportunities for growth.

To ensure a strong governance program, PTC maintains an Enterprise Cybersecurity Policy Management program (ESPM). This cross-functional team provides both management and users with a detailed understanding of the goals, approach and implemented controls for securing PTC Data and PTC Systems. This team ensures the governance is in place to protect sensitive and regulated information, including risk assessment, risk treatment, selection and implementation of security controls, ongoing evaluation and maintenance.

Through the policies and governance established via the ESPM, our programs provide assurances that PTC data and PTC systems are protected from unauthorized access, use, disclosure, duplication, modification, or destruction in order to maintain their confidentiality, integrity, and availability. To that end, the ESPM policies create a cross-functional cybersecurity framework that is aligned with industry standards such as:

- International Organization for Standardization's (ISO) publication 27001
- NIST Cybersecurity Framework (CSF)
- Cloud Security Alliance (CSA)
- Cloud Controls Matrix (CCM) and
- Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM)

Risk Assessment

PTC conducts an annual cybersecurity maturity assessment. Periodically, we engage a third-party security consulting firm to conduct an Enterprise Security Maturity Assessment. This independent assessment provides a mechanism to benchmark our current risk profile and enables us to measure progress as we make program improvements. Identified cybersecurity risks are reviewed by the Cybersecurity Strategy Council, which ensures that risk tolerances are established and used to appropriately manage risks.

Internal Auditing

Internal Audit is an independent assurance and advisory function with a direct reporting relationship to the PTC Board of Directors. The Internal Audit department conducts an annual organization-wide risk assessment that helps inform the annual audit planning process. The inputs for the risk assessment are interviews with key executives, enterprise-wide surveys, and various analysis of changing priorities processes and systems that could impact PTC achievement of its strategic and business objectives. In developing the internal audit plan, the processes and control activities by the 1st and 2nd lines, and results of third-party audits (among other inputs) are evaluated. All these factors are taken into consideration from a "Combined Assurance" perspective to develop Internal Audit's risk-based audit plan.

Third-Party Vendor Risk Management

The Vendor Risk Management (VRM) program supports PTC in meeting its Cybersecurity, Privacy, regulatory and compliance obligations and managing risk associated with Third-Party Vendors who have access to PTC IT Systems and Data.

Prior to outsourcing or allowing third-party access to PTC or customer systems, IP, or data; risks associated with such activity are clearly identified and documented. The process of selecting a third-party vendor includes due diligence of the vendor service or product in question in the form of a risk assessment based on publicly available information and the vendor's response to PTC's mandatory Cybersecurity & Privacy questionnaire and review of proposed terms and conditions to ensure that PTC is not exposed to unacceptable risk.

Third-party companies using PTC facilities (for example consultants), or accessing PTC's IT Systems are subject to PTC's VRM review and are required to demonstrate that proper security measures are in place before they have access to any PTC IT Systems or Data.

We ensure that all vendors that are approved by PTC's VRM process are contractually bound to maintain appropriate cybersecurity technical and organization measures and are bound to protect PTC's data that they may have access to.

Incident Response

PTC maintains a formal Cybersecurity Incident Response Policy. PTC follows this policy, its associated plans, and all contractual and regulatory requirements as applicable in any Cybersecurity Incident. The Policy is owned, enforced, and tested on a regular basis, including a continuous improvement program involving regular tabletop exercises. Cybersecurity Incident handling is managed by individual organizations with cybersecurity responsibility and monitored/guided by applicable corporate functions. All Cybersecurity Incident Response Plans are based on industry standards, such as the NIST Computer Security Incident Handling Guide – Special Publication 800-61.

PTC's Cybersecurity Incident Response Policy requires PTC to notify the affected customer without undue delay of an actual breach that affects the customer's data.

As it pertains to issues related to software delivered by PTC, please refer to the Technical Support section below.

TECHNOLOGY

IT Technical Controls

PTC's Cybersecurity infrastructure is made up of tools, technologies, and related processes that are deployed to protect the network perimeter and internal resources, including firewalls, intrusion detection, antivirus software, and internal access controls. PTC strives to implement and maintain best-in-class technology to protect our systems and devices.

Network and Endpoint Security

PTC IT uses next-generation firewalls with Intrusion Detection capabilities and maintains currency in order to ensure the firewall architecture remains robust. Firewall logs are monitored manually to ensure firewalls are not being tampered with. The DMZ architecture is multi-tiered and external networks and the DMZ server are monitored 24x7 for security violations.

PTC's IT strategy is to use content filtering to detect and prevent viruses from penetrating the perimeter and malware detection/protection as a second layer of defense to protect the desktop and file services.

Vulnerability scans are performed by in-house staff and are conducted regularly as well as immediately after potentially dangerous vulnerabilities are discovered or become publicly well-known.

Within our matrixed organization, depending on the nature of the product or environment, these internal penetration testing processes may be complemented by third-party penetration testing engagements.

- **IT Software Patching and Configuration Management:** All PTC IT Systems are subject to the patching program, which consists of monthly and out-of-cycle patching processes and procedures. Security patches are identified and prioritized on a continuous basis. Patches are implemented as appropriate, depending on the purpose, sensitivity, and potential vulnerability of the system.

  Only services that are required by a specific business need and that have been assessed for their impact on security are enabled.

  All changes that affect all IT systems and applications are expected to follow the documented change process and meet all process controls. A rollback plan is documented and tested as part of production change approval criteria. PTC has a systematic tool to log and archive changes. Changes recorded in this tool are retained for at least one (1) year.

Device Security

PTC IT uses industry-recognized endpoint protection software on all endpoints. PTC's Acceptable Use Policy requires that all employees leave anti-malware software installed and operational on corporate assets, and PTC IT monitors for compliance. Virus definition files or signatures are updated on a continuous basis. PTC also deploys virus scanning tools on our email servers. These tools are subject to periodic review and change. General use devices like employee laptops have controls in place including full hard drive encryption (where applicable) to protect all data.

PTC has Bring Your Own Device (BYOD) policies and mobile device use policies in place. Controls to protect access to PTC's IT Systems and Data are enforced through mobile application management and organizational controls. PTC leverages a mobile device management tool, which protects corporate assets when being accessed from mobile devices and includes remote-wiping capabilities. This tool is required for any employee wishing to use a BYOD.

PTC User Account Security

PTC requires the use of strong passwords for all systems in alignment with industry best practices and uses mechanisms to prevent the brute forcing of passwords. The requirements for service accounts meet or exceed user account requirements based upon the systems. Password vaulting is the standard for the most sensitive access situations. Multi-factor authentication is required for access to production environments as well as critical systems throughout the organization.

The IT Account Management Team is responsible for administering all user accounts, multi-factor authorization, and application accounts to authorized individuals. A unique user ID is in place for each user across PTC Systems and the network environment, governed by policy. User privileges are reviewed at least annually where applicable related to job function. Automated mechanisms are in place to disable user accounts upon termination. Access to PTC Systems is turned off immediately or within 24 hours. The Account Management Team follows set procedures for granting any business accounts requested for an employee. Accounts with permission beyond standard user accounts are granted based on authorization by the individual's manager – applying the principle of least privilege. Certain accounts, including HR and Financial systems, require a special set of approvals up to and including the department Vice President level.

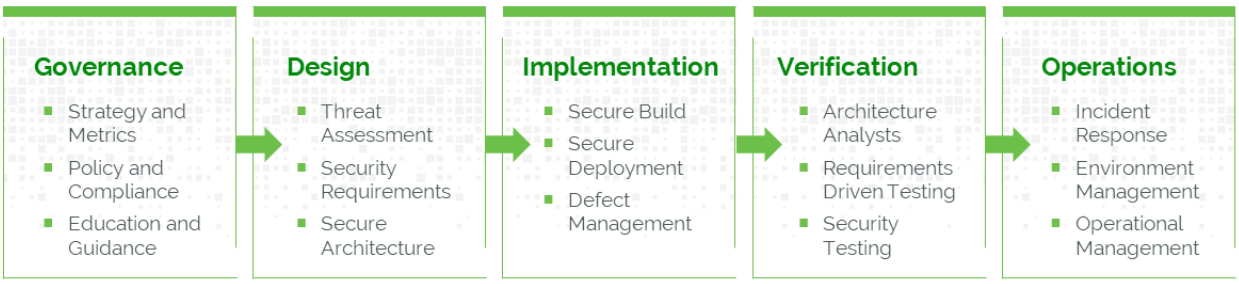
PTC Products and Services

Secure Software Development Lifecycle (SDLC) Program

Safety and security are incredibly important to PTC and to the ecosystems we serve. As we see greater convergence of physical and digital systems, we all carry a shared responsibility to develop and maintain more secure, defensible, and resilient systems. PTC is committed to doing our part through robust security programs and initiatives.

PTC's approach to creating secure applications is multi-leveled. As part of the Secure SDLC program, PTC follows the principle of security by design and uses automated scanning to prevent introduction of vulnerabilities into our products and environments. The Secure SDLC Program is built on the OWASP SAMM framework. At the core of this program, all developers are trained on application security risks (OWASP Top-10, CWE Top-25) to ensure code is fundamentally secure. Developers are required to attend application security awareness training at least annually. As part of our Secure SDLC Program, our policies and security practices include, but are not limited to, threat modeling, security design review, and vulnerability management.

PTC'S APPROACH TO CREATING SECURE APPLICATIONS IS MULTI-LEVELED



- **Product Vulnerability Disclosure Program:** PTC's Coordinated Vulnerability Disclosure (CVD) Program seeks contributions from external researchers who detect vulnerabilities in PTC's products. PTC invites both private individuals and organizations to report security vulnerabilities following a well-defined process that aligns with the National Telecommunications and Information Administration (NTIA) Safety Working Group's template. This program ensures that researchers can count on PTC's cooperation to protect its customers and the safety and privacy of the public. The CVD Program defines a framework for cybersecurity collaboration with customers, partners, and others within the industry. PTC supports the reporting and remediation of security vulnerabilities that could adversely affect the environments in which PTC products operate.

  Full details can be found here:
  https://www.ptc.com/en/documents/security/coordinated-vulnerability-disclosure

- **Product Privacy by Design and by Default:** Wherever appropriate, when developing its products and services, PTC follows the principles of Privacy by Design and by Default, and implements measures such as pseudonymization to enable adherence to the data privacy principles like data minimization.

PTC SaaS and Hosted Solutions

PTC's SaaS and Hosted Solutions are hosted through top-tier data center providers with world-class computing infrastructure that includes globally distributed, physically secure data centers with redundant power, cooling and networking. Perimeter protections include firewalls, web application firewalls, and IP filtering.

PTC's third-party hosting service providers have achieved multiple US and Internationally recognized security and quality accreditations including ISO 9001, ISO 27001, SOC 2 Type II, and NIST 800-53.

PTC's SaaS products have each achieved SOC 2 Type II compliance around their controls for Security, Availability, and Confidentiality (these reports can be requested from your sales representative). Communication between servers is monitored and restricted via virtual networks,

gateways and firewalls. Intrusion Detection systems are in place. Our cloud environments are continuously logged and monitored via a variety of rules and alerts that include configuration changes, login attempts, behavioral anomalies, and vulnerability scanning.

Data is encrypted in transit across public networks and at rest within our customer production environments.

PTC Administrators are required to leverage multi-factor authentication when accessing systems containing customer data.

For additional information on a specific PTC Cloud or SaaS product, please visit the following sites or request a copy of the SOC 2 Type II Attestation report for the relevant product(s) from your PTC contact.

- Onshape: https://www.onshape.com/security
- Arena: https://www.arenasolutions.com/security-platform/
- Vuforia: https://www.ptc.com/products/vuforia
- All other products hosted by PTC: https://www.ptc.com/-/media/Files/PDFs/Services/Cloud-Security-Whitepaper.pdf

Technical Support

PTC Technical Support offices are certified worldwide to ISO 9001 standards. This certification indicates our performance as a world-class support organization. This standard promotes consistent service, continuous self-improvement and a focus on customer satisfaction.

Successful certification means that all in-scope PTC technical support personnel adhere to a single set of carefully constructed processes and procedures in accordance with an internationally recognized standard and are validated by independent certification agencies. The result is that all customers receive the same quality of support from each of PTC's global Technical Support centers. Technical Support received its first ISO 9000 certification in 1999. In 2018 our certification was upgraded to the ISO 9001:2015 standard.

All information regarding updates or vulnerabilities impacting PTC products is available at https://ptc.com/support, and relevant notifications are automatically distributed to subscribed customers.

Business Continuity

Business Continuity Program

PTC has established Business Continuity Plans for SaaS and Hosted Solutions and Disaster Recovery Plans for critical information systems with a risk-based approach, in accordance with ISO27001 industry standards.

The plans establish the responsibilities, directives and recovery strategies for managing business continuity.

PTC takes a continuous improvement approach to its Enterprise Business Continuity Management System to ensure that our employees, stockholders, revenues, assets, clients, business relationships, corporate reputation, information, and information systems are properly protected from the impacts of a variety of risks typically classified as natural (e.g. weather-related, earthquakes, etc.), man-made (e.g. hackers, virus, theft, sabotage, workplace violence, financial attack, disinformation campaign, etc.), and technological (e.g. hardware failure, network failure, power outages, etc.).

PTC is in the process of attaining ISO22301 International Business Continuity Management Standard certification.

The program is governed by a cross-functional team of Business leaders with Executive Leadership oversight, led by the Business Continuity Manager.

Privacy

PTC considers the protection of personal information as a fundamental human right. As such, PTC has developed and implemented a global Privacy Program to safeguard personal information through sound policies and procedures that place appropriate controls on personal information processing. The PTC Privacy Program applies the 6 Principles Relating to the Processing of Personal Data (as set out in GDPR) to all processing of personal information globally. PTC's SVP Global Data Privacy Officer draws on appropriate resources to meet the goals and the priorities of the Privacy Program. The Program has been appropriately designed to address both global and local Privacy requirements and to adhere to the Privacy Principles. PTC seeks to ensure that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing of personal information, as well as the risk, PTC maintains appropriate technical and organizational measures to ensure a level of Cybersecurity appropriate to the risk.

Compliance with International Data Privacy Legislation

PTC complies with all applicable privacy regulations wherever we do business. As PTC is a global company, personal data may be accessed anywhere in the world by PTC Enterprise Employees to ensure that all systems and services maintain the highest possible availability and efficiency of

delivery. The majority of PTC Systems are hosted in the USA. PTC's AWS and Azure Cloud Services are managed by PTC Inc in USA and PTC India in Pune. PTC's technical support is provided by PTC Affiliates and subcontractors in EMEA, USA, India, China and Japan.

International Transfers of Personal Information

Each of PTC Inc.'s EU, Swiss and UK Affiliates has appointed PTC Inc. and other PTC Affiliates as its sub-processors. PTC has put in place a Global Data Transfer Agreement, based on the EU Commission's Standard Model Clauses (Commission Decision (EU)2021/914) covering the transfer and processing of all personal information by the PTC Enterprise to ensure appropriate safeguards are in place when transferring personal information to countries that the European Commission does not consider as providing adequate protection of personal information. PTC has also implemented supplemental measures such as encryption of personal information in transit and when at rest. PTC has initiated the process to apply for approval by the EU Data Processing Authorities of the Binding Corporate Rules (BCR) and anticipates having BCRs approved.

All third-party sub-processors appointed by PTC Inc have signed terms equivalent to the Standard Contractual Clauses (SCC).

Please see the Schedule to PTC Group's Data Processing Terms & Conditions available on PTC's Privacy Page at https://www.ptc.com/documents/policies. Also, please see PTC's Privacy Policy at https://www.ptc.com/documents/policies/privacy or contact PTC's Global Data Privacy Officer at dataprivacy@ptc.com.

Product Data Collection

In order to understand how our software is used, how it performs, and the preferences of the users, PTC may use various methods and tools to collect data on the use and performance of the Software. Data items like hostnames, IP addresses, ports, and user identifiers are anonymized before they are transmitted to PTC.

Product telemetry can offer insights on feature usage, proactive resolution of issues, improved license compliance management, and offering better visibility into performance without the need to solicit feedback directly from users. PTC respects and values the trust that customers place in PTC and uses this data for the purposes of improving our products and the customer experience.

DIGITAL TRANSFORMS PHYSICAL

PTC, Inc.

2022

www.ptc.com