# Cybersecurity White Paper

## PTC Security and Governance Framework

### Corporate Security Approach

PTC employs a holistic, multi-layered cybersecurity and privacy program grounded in Zero Trust principles—assume breach, verify explicitly, enforce least privilege, and continuously monitor. In a globally connected environment where every entry point is a potential risk, PTC secures what we control and partners with suppliers and customers to maintain strong patching, device hygiene, and credential protection.

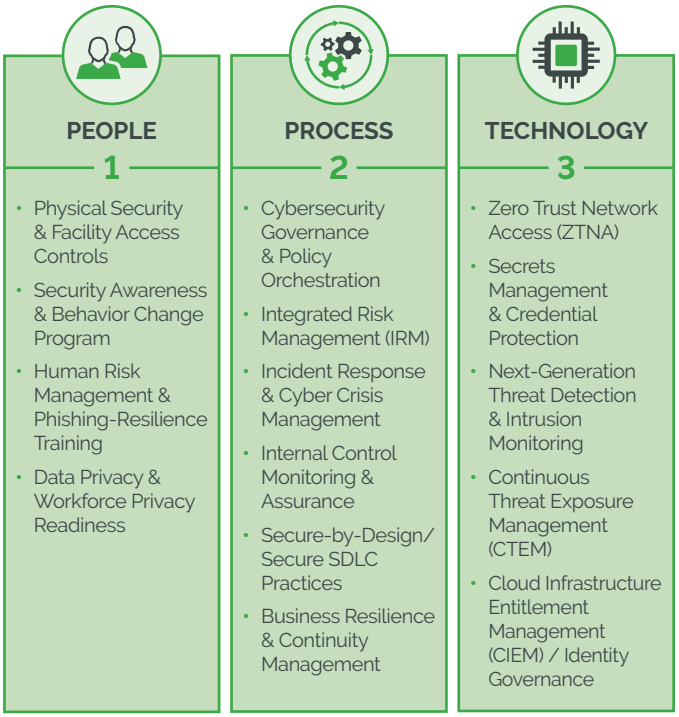
- **People:** PTC recognizes that technology alone cannot mitigate all security threats, and so we focus on developing our most critical resource: our people. Security is the responsibility of every PTC worker and is independent of departmental affiliation. PTC's corporate cybersecurity awareness activities 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 leverages technology to automate security controls and reduce human error wherever possible. 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.

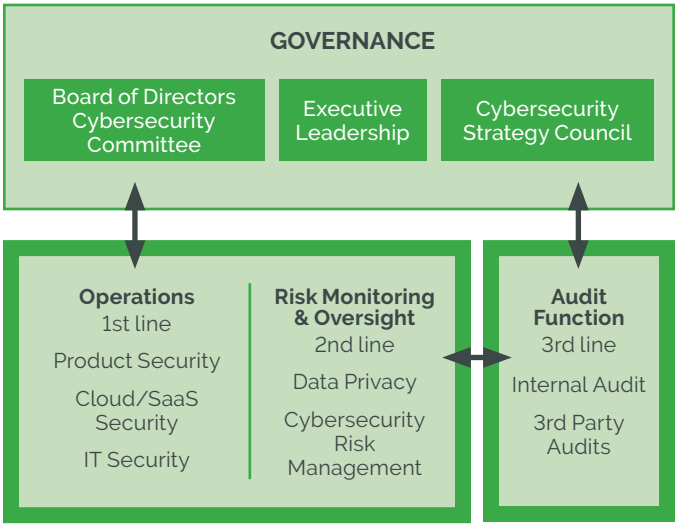
These three key elements of People, Process, and Technology are tightly interwoven to secure our environments and data.

**PTC's Cybersecurity Landscape**




## 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 on a quarterly basis.




The Three Lines model is defined as follows:

- **Operations (1st line):** The 1st line Operational Management of an organization is responsible for implementing 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 establishes policies and provides knowledge to support the 1st line. It oversees the controls implemented by the 1st line by performing routine monitoring of the risk, ensuring that controls are properly designed and operating effectively.
- **Audit Function (3rd line):** The 3rd line independently evaluates the effectiveness of risk management, controls, and governance processes implemented by the 1st and 2nd lines. PTC's Internal Audit team coordinates with external auditors to ensure comprehensive audit coverage.

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.

Document Control and Management is performed in the central Governance, Risk, and Compliance tool. Exceptions to policies are documented in the appropriate system of record.

## Compliance

PTC's Cybersecurity Program is supported by robust processes and procedures at all levels. Our matrixed cybersecurity organization is governed by industry-standard frameworks, including:

- International Organization for Standardization's (ISO) publication 27001 and 9001
- NIST Cybersecurity Framework (CSF)
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
- Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM) and Secure Software Development Framework (SSDF)

As a public company, PTC also requires a full cycle of SOX compliance activities that include everything from design to tests of operating effectiveness of business and IT controls by management, internal audit, and our external auditors.

### Cyber Risk Management

PTC's Cyber Risk Management department maintains a central cyber risk register in the Governance, Risk and Compliance platform. Cyber Risks are managed throughout their lifecycle, including identification, assessment and scoring, and assignment of treatment plans that are regularly reviewed in periodic meetings with domain security leadership.

To measure the effectiveness of risk remediation efforts and identify any new risks, 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.

### Third-Party Vendor Risk Management

The Vendor Risk Management (VRM) program has been established to support 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. VRM is led by a dedicated VRM Program Manager reporting to the Chief Compliance Officer.

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's service or product in question in the form of a risk assessment based on publicly available information, including third-party accreditations, audit reports, security and privacy policies, along with the vendor's response to PTC's Cybersecurity & Privacy questionnaire to ensure that PTC is not exposed to unacceptable risk.

Due diligence is performed on all vendors, and each is then reviewed for:

- PII handling and processing by Data Privacy
- Cybersecurity by Information Security
- Information Technology requirements by IT Logistics
- Terms, conditions and security requirements by Legal
- Overall policy and process adherence by the VRM Program Manager

Vendors are then periodically reassessed according to their assigned Tier based on the criticality of the service and sensitivity of data accessible to them. Tier 1 Critical vendors are reassessed annually.

Vendors whose software incorporates Artificial Intelligence (AI) technology are required to meet additional criteria in a separate dedicated review process.

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 and data privacy 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 organizational measures and are bound to protect PTC's Data that they may have access to.

A list of PTC's sub-processors can be found here: https://www.ptc.com/documents/legal-agreements/data-processing-terms-and-conditions.

# People

## Physical Security

PTC operates in controlled-access facilities and has established Global Security Policies and Standards. 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. Restricted areas such as data centers, network rooms and similar areas containing IT and other sensitive resources shall be restricted to authorized personnel only, using appropriate entry controls to limit and monitor physical access. Facility access lists are reviewed quarterly by local office managers/administrators to ensure the access roster is accurate and only those with the current business need for access are included. All PTC facilities maintain Emergency Action Plans (EAP), detailing emergency contact numbers, assembly, shelter in place locations, PTC volunteer emergency responders. All PTC EAP's provide facility level guidance pertaining to workplace emergencies, including bomb threats, medical emergencies, severe weather, natural disasters, power failure, workplace violence, and fire prevention and response.

## 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. Further resources are made available to employees for career and professional development. All employees undergo an annual Performance Evaluation review.

## Worker Commitments

PTC employees are contractually committed to protecting and preserving the confidentiality and integrity of PTC information and systems under their terms of employment. Background checks at PTC are performed during the evaluation process for all new hires. As part of PTC's hiring practices, we qualify applicants by performing education, previous employment verification, reference checks, and other relevant checks based on the desired position. Where Laws or Regulations permit, PTC conducts criminal background checks.

PTC has both an Acceptable Use Policy (AUP), and an Information Security Policy that apply to all individuals accessing PTC internal systems. All new employees must acknowledge that they have read, understand, and agree to abide by the rules of behavior in the Acceptable Use Policy, which is provided to them 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 workers, which includes PTC employees and workers who have access to internal PTC Assets. Among other controls, PTC's AUP requires that workers adhere to Clean Desk and Clear Screen procedures. The policy includes a disciplinary process for policy violations.

## Cybersecurity & Privacy Training and Awareness

PTC is responsible for ensuring all PTC Employees receive regular cybersecurity training and awareness. PTC's Cybersecurity Training and Awareness Program includes: 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 PTC identifies such a need during the annual enterprise risk assessment or after a cybersecurity Incident, PTC will supplement training with emails, posters, or activities.

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

- PTC 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's 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 course that includes cybersecurity topics such as malware, phishing, trojans, social media.
- PTC uses a trusted third-party vendor to conduct an email phishing simulation program. All users receive a simulation at least annually, and remedial training is assigned where required.
- Lastly PTC has a cybersecurity awareness program that covers incremental topics based on current events such as the safe use of AI tools.

# 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 Security Architecture**

PTC IT maintains next-generation firewalls with Intrusion Detection/Prevention capabilities to ensure the firewall architecture remains robust as a part of its Zero Trust Network Architecture. Firewall logs are monitored to ensure firewalls are not being tampered with. The DMZ architecture is multi-tiered and external networks, and the DMZ servers are monitored 24x7 by PTC Security Operations.

PTC's IT strategy is to use content inspection 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 as further detailed below.

Network vulnerability scans are performed by automated systems, reviewed 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, internal network penetration testing processes are performed regularly and complemented by at least annual third-party penetration testing engagements.

PTC's enterprise email service implements industry-leading security controls, including advanced filtering, encryption in transit and at rest, continuous monitoring, message quarantining, and enforcement of sender authentication protocols (SPF and DMARC configured to reject) to mitigate risks of phishing, spoofing, and unauthorized access.

## 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 with this and other Acceptable Use Policy provisions. PTC uses a modern endpoint and server protection system that uses real-time threat intelligence, behavioral analysis, and machine-learning–based detection. This means it identifies and blocks threats automatically without needing regular definition updates. General use devices like employee laptops have controls in place including full hard drive encryption (where applicable) to protect all data.

PTC endpoint devices are only allowed to connect to PTC internal networks via PTC's Zero Trust Network Access solution, which replaces and exceeds the role of a traditional VPN solution. PTC endpoint devices are only allowed to connect to sanctioned external systems via PTC's Zero Trust Network solution, which performs outbound intrusion detection and prevention.

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. When PTC is made aware of industry-critical patches, they are prioritized above all else.

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.

PTC has 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 mobile device.

## PTC User Account Security

PTC requires the use of strong passwords for all systems in alignment with industry best practices, including NIST recommendations, 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 involving privileged account identities. Multi-factor authentication is required for access to PTC systems in the internal network.

The Identity and Access Management Team is responsible for administering all PTC worker accounts used for Single Sign-on (SSO). A unique user ID is in place for each PTC worker across PTC systems and the network environment, governed by policy. Access 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 Identity and Access Management Team follows set procedures and obtains approvals from respective business application owners for granting any business account access requested for a worker, while 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.

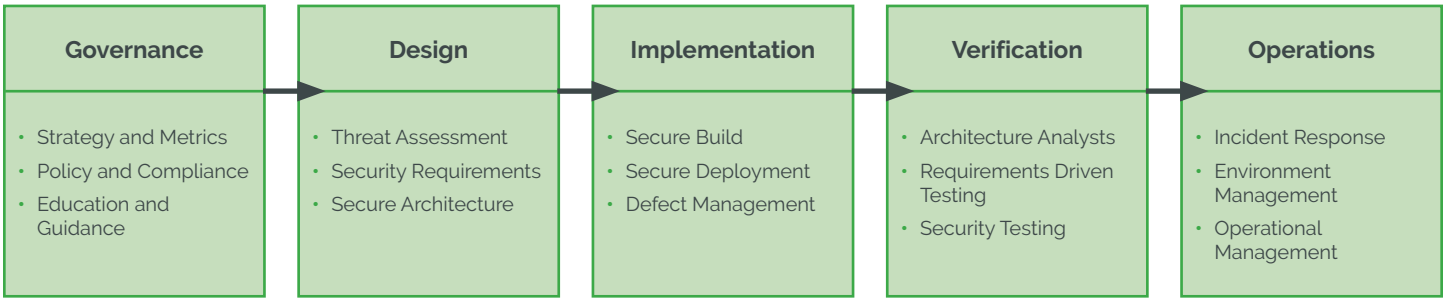
## PTC Product Security

**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.

As part of the Secure Software Development Lifecycle (SDLC) program, PTC follows the principle of security by design and uses both automated scanning and manual penetration testing to prevent introduction of vulnerabilities into our products and environments. Automated scanning includes, but is not limited to, static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), and malware scanning. SCA is also performed on all open-source components shipped with PTC products, and Software Bills of Materials (SBOMs) can be produced. 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/SANS 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 reviews, security code reviews and vulnerability management. For any vulnerabilities, PTC will address security vulnerabilities in a manner and timeframe consistent with industry best practices and in line with PTC's SDLC policies.

**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. PTC has also been accepted as a Certificate Numbering Authority (CNA) by the US Cybersecurity and Infrastructure Security Agency (CISA) in recognition of our strong program and partnership. A CNA is an authorized entity with specific scope and responsibility to regularly assign CVE IDs and publish corresponding CVE Records. 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 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, and SOC 2 Type II.

PTC's SaaS products have each achieved SOC 2 Type II compliance around their controls for Security, Availability, and Confidentiality 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 Personnel are granted access according to least privilege, and PTC Administrators are required to leverage multi-factor authentication when accessing systems containing customer data.

For additional information on a specific PTC SaaS or Hosted solution, please request the relevant SOC 2 Type II Attestation report through this form on the PTC.com Trust Center: https://www.ptc.com/about/trust-center/soc2.

## 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.

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. Existing customers can manage notifications in PTC's eSupport Portal: https://support.ptc.com/appserver/cs/subscriptions/subscriptions.jsp?p=tab_bulletins.

## Artificial Intelligence

PTC is committed to responsible and ethical use of AI across both our products and our internal operations. To guide this work, we have established an AI Action Committee and an AI Steering Committee that evaluate AI-related risks and benefits and define the processes that support responsible AI use throughout the company.

Transparency is a core principle of PTC's AI approach. We maintain clear visibility to:

- How AI is used in our business operations and product development
- Where AI capabilities appear in our products and how they align with trustworthy-AI principles
- What data is available to AI systems and how that data is processed

As part of our Vendor Risk Management program, PTC has created a dedicated workstream to evaluate internal tools that include AI functionality. We require our AI vendors to meet the same privacy and security standards that we uphold for our own AI products. We only use solutions built on reputable AI models that ensure our data remains private and secure, and these vendors are reviewed on a regular basis.

PTC empowers employees to use AI responsibly to improve productivity. All employees receive training in responsible AI practices during onboarding, with additional role-specific training provided as needed.

PTC recognizes the significant value AI brings to modern businesses and incorporates this technology into the solutions we provide. PTC uses industry-leading, pre-trained models from reputable vendors such as Microsoft and AWS in the development of our AI solutions. Customer data is not used to train AI models without explicit consent. In the context of Large Language Models (LLMs) and AI-enabled product features, PTC Product Security is actively involved to ensure these technologies are developed, deployed, and maintained securely and responsibly. All code—whether written by developers or generated by AI—undergoes the same rigorous security testing and review processes established in PTC's Secure Development Lifecycle (SDLC). This includes protections against emerging AI-related threats such as model manipulation, prompt injection, data leakage, adversarial inputs, and unauthorized access to sensitive training data or outputs, in accordance with the PTC Policy on the Use of AI-Generated Code in PTC Software.

Product Security plays a critical role in:

- Safeguarding application integrity and authenticity
- Ensuring secure integration of AI into broader software ecosystems
- Mitigating risks from third-party AI components and APIs

Embedding security throughout the AI product lifecycle helps build customer trust, reduce risk, and support regulatory readiness in an evolving threat landscape.

PTC remains deeply committed to the responsible, transparent, and secure use of AI across our products, development processes, and day-to-day operations. By embedding ethical practices, rigorous security controls, and strong governance into every stage of our AI lifecycle, we ensure that AI technologies are used in ways that protect our customers, support our employees, and uphold the highest standards of trust and accountability.

# Cyber Resilience

## Cyber Incident Response

PTC maintains a formal Enterprise 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 by Cybersecurity Compliance through 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.

## Business Continuity

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 and established SOC 2 controls.

The plans establish responsibilities, directives and recovery strategies for managing business continuity and are tested annually.

PTC takes a continuous improvement approach to Business Continuity and Resiliency 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 maintains plans that are regularly tested to ensure business continuity and resiliency of systems that support IT general controls in accordance with PTC's

SOX compliance. We leverage industry best-in-class SaaS products to provide us with ongoing resilience in our enterprise space managed by a robust VRM process. We use an automated disaster-recovery orchestration platform that continuously replicates critical systems and configurations. In the event of an outage, this platform enables us to rapidly restore services by provisioning replacement infrastructure, applying the most recent backups, and validating system integrity. This ensures that recovery is consistent, repeatable, and aligned with our Recovery Time and Recovery Point Objectives (RTO/RPO).

## 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 (CCPA, CIPP) 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, such as those in the United States and Canada, 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. PTC has a program to continuously review changes to our policies to enable compliance with evolving regulations, supported by industry organizations such as the International Association of Privacy Professionals (IAPP). 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. The following types of personal information may be processed in order to provide the service: Name, UserID/ User-name, Company, organization, business contact details, interactions with PTC's products and services such as log-files and incident reports, data that may be processed by PTC's products (such as IP addresses, cookie data, device identifiers and similar device-related information), and any other personal information that may be uploaded by Customer to the PTC service.

Collection of personal information does not happen in addition to the normal interaction as part of the provision of PTC's products and services.

### 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.

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

Please see the PTC Cybersecurity and Data Privacy Addendum (DPA) at https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions as well as PTC's Privacy Policies at https://www.ptc.com/documents/policies/privacy or contact PTC's Global Data Privacy Officer at contact dataprivacy@ptc.com.



1039150_Cybersecurity_Whitepaper_01_26