



UST PACE Platform – Service Definition

Version: 3.0

Status: Approved

Owner: PACE Product & Platform Engineering

Service Type: Platform Engineering / DevSecOps Enablement

Last Updated: January 2026

1. Document Control

Version	v3.0
Author	PACE Product Engineering Team
Reviewers	PACE Platform Leadership
Approval	Martin Parker

2. Purpose

This document defines the **PACE Platform Engineering Product**, including:

- Service scope and capabilities
- Deployment and operational model
- Security, compliance and governance
- Support model and service levels
- Customer responsibilities and boundaries

The goal is to provide clear expectations, assurance, and transparency for customers adopting PACE.

The document is intended for customer stakeholders, procurement, security and delivery teams.

3. Service Overview

3.1 Service Description

UST PACE is a cloud-based Platform Engineering and Delivery Governance platform that provides a unified control plane across an organisation's software delivery toolchain. It enables organisations to standardise how services are designed, built, released and operated while retaining freedom of choice in underlying tools. It provides:

- Standardised onboarding and delivery frameworks
- Secure DevSecOps enablement and governance
- Delivery, compliance and operational visibility
- Governance and operational guardrails

UST PACE is designed around Platform Engineering, DevSecOps and Site Reliability Engineering (SRE) principles, providing government organisations with predictable delivery, assured compliance, and full operational traceability across the software lifecycle.

4. Service Scope

4.1 In Scope

The PACE service includes:

Platform Capability

- **Platform engineering and delivery governance control plane**
A unified layer that connects and governs source control, CI/CD, security, infrastructure and environments.
- **Policy-driven DevSecOps orchestration**
Enforcement of security, quality, compliance and release controls across existing CI/CD pipelines and toolchains.
- **Standardised onboarding and delivery blueprints**
Golden paths, templates, and approved patterns that ensure teams adopt compliant ways of working from day one.
- **Environment and release governance**
Controls for environments, approvals, separation of duties, and promotion rules across development, test and production.
- **Delivery, compliance and operational insight**
Federated visibility across pipelines, security, cost, and environments for audit, risk and readiness reporting.
- **Toolchain integration and federation**
Secure integration with source control, CI/CD, security tooling and cloud to provide end-to-end delivery governance

Operational Services

- Platform onboarding and tenant setup
- Configuration guidance and best-practice adoption
- Platform operation, maintenance and upgrades
- Product training and embedded help
- Support and incident management as defined in SLAs

4.2 Out of Scope

The following activities are not included in the PACE service unless explicitly contracted:

- Customer application development or feature delivery
- Operation or administration of customer cloud infrastructure or production environments
- 24x7 production incident management for customer applications
- Bespoke tooling or integrations not aligned to the PACE product roadmap
- Customer-specific platform forks or non-standard modifications
- Organisational change management, workforce transformation, or process re-engineering
- Operational monitoring and application performance management (APM)

4.3 Customer Responsibilities

Customers remain responsible for:

- Providing PACE with the necessary access to approved toolchains and environments (e.g. source control, CI/CD, cloud accounts, security tools)
- Operating and securing their application workloads and cloud environments
- Owning, maintaining and deploying their application code
- Responding to security findings, compliance violations and policy breaches identified by PACE
- Following the operational standards enforced by the PACE platform

5. Target Users & Industries

PACE supports:

- Enterprise Organisations
- Mid-Market Businesses
- High-Growth Technology Teams
- Start-ups scaling delivery

Applicable industries include technology, financial services, healthcare, manufacturing, public sector, and regulated industries requiring compliance and secure delivery.

6. Deployment Model

6.1 Supported Environments

PACE supports deployment in:

- Public Cloud (AWS, Azure, GCP)
- On-Premise & Private Cloud

6.2 Deployment Responsibility Model

Model	Hosted By	Managed By	Typical Use
SaaS	UST	PACE Platform Team	Rapid adoption
Customer Hosted (on Kubernetes)	Client	Shared Responsibility	Compliance-driven

In all models, customers retain ownership of their code, cloud accounts and production environments.

7. Technical Architecture Summary

PACE is built on modern cloud-native principles including:

- Kubernetes-based orchestration
- Containerised services
- Secure integration with CI/CD tooling
- Dynamic scaling
- Resilience and high availability
- Identity and access integration with customer IdPs (e.g. Azure AD, Okta, Ping)

PACE is tool-agnostic and integrates with leading DevOps, SCM, security and cloud platforms.

8. Features

Standardised onboarding and delivery accelerators

Golden paths, templates and blueprints for compliant, repeatable team onboarding.

Toolchain-agnostic platform framework

Works across GitHub, GitLab, Jenkins, cloud providers and security tooling without locking customers into a single stack.

Policy-driven CI/CD orchestration

Enforces how pipelines, approvals, environments and releases operate — without replacing existing CI/CD engines.

Delivery, risk and operational insight

Federated visibility across pipelines, security and environments for audit, readiness and governance.

Governance with team autonomy

Teams retain self-service delivery while platform rules ensure consistency, safety and compliance.

Improved release flow and reduced lead time

Standardisation and automation remove friction between build, test and production.

9. Business Benefits

- Faster, more predictable software delivery
- Reduced delivery, security and compliance risk
- Higher developer productivity through self-service platforms
- Built-in DevSecOps and compliance assurance
- Measurable improvements in delivery performance (e.g. DORA metrics)
- Improved service stability and release confidence

- Reduced rework and delivery waste

10. Security & Compliance

PACE is designed as a secure, policy-driven platform control plane that integrates with customer toolchains and environments while enforcing security, compliance and governance standards.

Security Controls

- Role-based access control (RBAC)
- Secure secrets and credential integration (e.g. integration with customer-approved secret stores and identity providers)
- Policy-as-code enforcement - Controls governing pipelines, environments and approvals
- Security, quality and compliance toolchain integration. Orchestrates and enforces the use of approved scanning and testing tools within CI/CD workflows.

Compliance Alignment

- GDPR and UK GDPR considerations
- Logging and audit traceability
- Secure handling of platform metadata and configuration data

PACE does not host or process customer application or production data. It stores only the minimum configuration, metadata and audit information required to operate the platform.

11. Service Operations

11.1 Support Model

- **Coverage:** 16 hours per day, 5 days per week
- **Support Channels:** Dedicated Support via Email / Ticketing
- **Optional Enhancements:** Collaboration channels subject to agreement

Support relates to the **PACE platform and integrations**, not to customer applications or cloud infrastructure.

11.2 Service Levels

Severity	Example	Response Target
Critical	Platform Unavailable	1 hour
High	Major Feature Failure	4 hours
Medium	Functional degradation	Within 24 hours
Low	Queries, Minor Issues	2-3 business days

Resolution times depend on issue complexity and cooperation with customer toolchain providers.

Third-party platform outages (e.g. GitHub, cloud providers) are excluded from SLA measurements.

12. Upgrades & Release Policy

- Monthly feature releases
- Security and hotfix updates as required
- Planned maintenance communicated in advance
- Backward-compatibility of published APIs and templates will be maintained where reasonably practicable.

Upgrades do not modify customer pipelines or environments

13. Training & Enablement

- Embedded in-platform help
- Optional enablement workshops
- Optional adoption support programmes

14. Reporting & Continuous Improvement

PACE provides federated visibility across the delivery toolchain to support governance, assurance and continuous improvement:

PACE Supports:

- **Delivery performance and trend reporting**
(e.g. flow, throughput, release cadence, failure rates)
- **Compliance, risk and operational insight**
Across pipelines, environments, security and approvals.
- **Continuous feedback loops**
Using data from CI/CD, security, quality and cost tooling to improve delivery outcomes.

15. Exit & Offboarding

If a customer exits the service:

- PACE access will be revoked in a controlled and auditable manner
- Customer-owned code, data and cloud assets remain the property of the customer

- Configuration, audit data and platform metadata will be made available for export within an agreed period
- Transition support will be provided within the contracted scope
- All customer data and metadata will be deleted from UST systems in accordance with the agreed data retention policy.

16. Assumptions & Constraints

The PACE service is provided on the basis that:

- Customers provide timely access to required toolchains and environments
- Service performance depends on the availability of third-party tools and platforms (e.g. GitHub, cloud providers).
- Bespoke or non-standard requirements require separate commercial and technical agreement.
- PACE does not guarantee delivery outcomes, only the operation of the platform and its controls.

17. Acceptance

Use of the PACE product constitutes acceptance of this Service Definition and any associated contractual terms governing the service.