Internal Developer Platform SaaS (Port.io) – Service Definition

G-Cloud 15 Lot 2a – Infrastructure Software as a Service (ISaaS)

Document control

Service name: Internal Developer Platform Software as a Service (SaaS) (Port.io)
Supplier name: Lean Tree Ltd
Version: v1.0
Date: 23 January 2026
Status: Final

1. Service overview

Outcome: A usable internal developer platform capability that improves service ownership visibility and enables approved self-service workflows without building a bespoke portal.

How: Provided as a hosted SaaS platform with onboarding and configuration support, enabling catalogue setup, workflow templates and integration with buyer tooling where available.

Boundary: The underlying SaaS is provided by the vendor; bespoke product development is out of scope. Integration and configuration scope is agreed at call-off; the buyer remains responsible for their cloud resources and access approvals.

Who it is for: Platform, infrastructure, development and operations (DevOps), security operations (SecOps) and engineering teams.

Buyer needs met: Manage, monitor, optimise, or secure infrastructure using a SaaS platform and associated onboarding/support.

Service model: Port (port.io) hosted SaaS accessed over the public internet using Hypertext Transfer Protocol Secure (HTTPS). Tenant model is defined by Port (port.io) and may include multi-tenant or dedicated tenant options, subject to commercial agreement.

2. What this service covers (Lot 2a scope)

Included capabilities:

- Central software and service catalogue with ownership metadata
- Self-service workflow catalogue for approved tasks (golden paths)
- Templates for scaffolding and standardising new services

- Scorecards and policy checks for standards and compliance
- Tool integrations for source control, Continuous Integration/Continuous Delivery (Continuous Integration (CI)/Continuous Delivery (CD)), incident, and observability
- Role-based access control and audit logging
- Accessible User Interface (UI) compliant with Web Content Accessibility Guidelines (WCAG) 2.2 (Level A & AA), Section 508 and EN 301 549

Supported target environments: Yes. The service can integrate with multiple cloud providers through buyer-controlled accounts and APIs. Cloud resources remain provisioned and owned in the buyer environment. The portal provides a consistent interface for workflows and standards across different cloud platforms, subject to the integrations configured by the buyer.

Integrations and connectors: Web-based management interface and Representational State Transfer (REST) Application Programming Interface (API). Webhooks may be available to integrate with external systems, subject to Port (port.io) capability. The Internal Developer Platform (IDP) provides a REST API for catalogue management, workflows/actions and administration. It features REST API authentication using JSON Web Token (JWT) tokens generated from account API credentials (client ID/secret).

Out of scope: No bespoke development of the underlying SaaS product. Procurement of any third-party licences is out of scope unless explicitly included at call-off.

3. Service description and features

Key features:

- Central software and service catalogue with ownership metadata
- Self-service workflow catalogue for approved tasks (golden paths)
- Templates for scaffolding and standardising new services
- Scorecards and policy checks for standards and compliance
- Tool integrations for source control, CI/CD, incident, and observability
- Role-based access control and audit logging
- Accessible UI compliant with WCAG 2.2 (Level A & AA), Section 508 and EN 301 549

Admin and operator functions: Configurable taxonomy, templates, workflows, scorecards, integrations, and Role-Based Access Control (RBAC). Deep custom development is out of scope unless provided as a separate professional service. Online documentation and guided onboarding are provided. Support includes ticketing, knowledge articles, and scheduled sessions for administrators during initial configuration.

Automation and policy-as-code: The IDP provides a REST API for catalogue management, workflows/actions and administration. It features REST API authentication using JWT tokens generated from account API credentials (client ID/secret).

Reporting, dashboards, and exports: Metrics and reporting may include catalogue completeness, workflow runs, template usage, scorecard results, and administrative or audit events. Reports are available via the interface and may be exportable. Export is provided through the service interface and API. The export scope includes catalogue records, configuration, and audit information where available. The buyer can schedule exports prior to termination.

4. Service provisioning and onboarding

How buyers start using the service: 1. Create tenant and administrator accounts 2. Configure authentication and user groups (Single Sign-On (SSO) where required) 3. Connect integrations (source control, CI/CD, ticketing, cloud accounts) 4. Import or define services and ownership metadata 5. Configure templates, workflows, and scorecards 6. Run pilot onboarding with a small set of teams before wider rollout

Information required from buyer: Scope and configuration inputs are confirmed at call-off.

Access requirements: Requires outbound HTTPS access from buyer networks to Port. Data ingestion uses push-based methods; inbound connectivity to buyer environments is not required for ingestion. For customers with strict network controls, on-premises Ocean integrations can be deployed in the buyer environment so data can be processed locally and only required results sent to Port. Onboarding timelines depend on integration complexity and buyer readiness; mobilisation is agreed at call-off.

Typical onboarding timeline: Onboarding timelines depend on integration complexity and are agreed at call-off.

5. Support, service levels, and incident management

Support hours and channels:
Support is provided via email/ticketing with service hours and escalation routes agreed at call-off. Lean Tree provides onboarding support, incident triage and coordination with the vendor where required. Response targets, service hours and any enhanced support options are confirmed and priced during discovery and scoping, then documented in the call-off contract.

Incident management: Incidents are logged, prioritised and handled through defined processes with triage, escalation and stakeholder updates agreed at call-off. Where a security incident affects buyer data, Port notifies customers as soon as possible and provides periodic updates during the day covering progress and impact. Response and resolution targets and any service levels are confirmed and priced during discovery and scoping, then documented in the call-off contract.

Buyer notifications: Notification and reporting timescales are agreed at call-off based on the buyer's incident-management process and reporting needs.

Change and release management: Changes are requested, assessed for impact and risk, approved, implemented, and reviewed. Buyer-facing configuration changes follow buyer approval. Port (port.io) platform changes follow Port (port.io) release controls. Integrations and workflows are version controlled where possible.

6. Security and data protection

6.1 Data protection between buyer and supplier

Protection between networks: Data in transit is protected using encryption provided by the underlying service and standard secure transport mechanisms. Details can be provided in service documentation.

Protection within supplier network: Within Port (port.io) environment, network segmentation and access controls are applied to separate tenants and restrict administrative access. Details are provided in Port (port.io) security documentation.

6.2 Data storage and processing

Data storage locations: Port is hosted on Amazon Web Services (AWS). Data storage and processing locations depend on the service region selected and the vendor sub-processors in use. Port maintains a published sub-processor list and provides a Data Protection Addendum (Data Protection Act (DPA)). Specific sub-processor names, purposes, and change-notification methods are confirmed at call-off against the latest Port.io product/security documentation and applicable subscription terms. Cross-border processing/transfers are governed by the DPA.

Data processing locations: Processing locations follow the underlying SaaS service and buyer contract, confirmed at call-off.

Sub-processors: Sub-processors are defined by the SaaS vendor and confirmed at call-off.

Data retention: Log retention periods are configurable and agreed with the buyer, subject to the underlying service capabilities.

6.3 Encryption and key management

Encryption in transit: Data in transit is protected using encryption provided by the underlying service and standard secure transport mechanisms. Details can be provided in service documentation.

Encryption at rest: Data at rest is protected using encryption provided by the underlying service and platform capabilities. Details can be provided in service documentation.

Key management model: Key management is provided by the underlying SaaS platform and hosting provider. Buyer-specific requirements are agreed at call-off.

6.4 Vulnerability, testing, and assurance

Vulnerability management: The IDP Port (port.io) uses tooling such as Snyk (dependency vulnerability scanning), Trivy (container vulnerability scanning), and Semgrep (Static Application Security Testing (SAST)). They also publish a vulnerability remediation timeline by severity (e.g., Critical within 30 days, High within 60 days, Medium within 120 days, Low within 180 days). The IDP undergoes annual third-party penetration testing; a summary of findings is available upon request.

Penetration testing: The Port (port.io) undertakes penetration testing and vulnerability assessment on a regular basis. Summary outcomes and remediation approach can be provided under appropriate terms. Testing cadence is confirmed with Port (port.io).

Remediation: Remediation actions are tracked and closed using the agreed action log and governance cadence.

6.5 Identity and access management

User authentication methods: Port supports buyer single sign-on (SSO) using external identity providers via OpenID Connect (OIDC) and Security Assertion Markup Language (SAML) 2.0. Where configured, authentication (including Multi-Factor Authentication (MFA) policies) is enforced through the buyer identity provider. Port can sync users and teams/groups on sign-in (identity provider dependent). Port does not fully support System for Cross-domain Identity Management (SCIM) provisioning at this time; SCIM requirements are confirmed at call-off against the latest Port.io product/security documentation and applicable subscription terms.

Privileged/admin access controls: Administrative access is restricted to authorised roles using least privilege. Support access is controlled through ticketing systems with appropriate authentication and auditability. Privileged actions are logged.

Access reviews: Access controls are reviewed regularly and on material change. Frequency is at least annually, and more frequently where required by policy or buyer risk.

6.6 Audit logging

Buyer user action audit: The service provides audit logs for buyer user actions such as authentication events, configuration changes, and workflow executions, subject to Port (port.io) capability. Buyers can access audit logs via the interface and, where available, export or API.

Supplier admin action audit: Administrative and support actions performed by supplier users are logged within the relevant systems, subject to Port (port.io) capability. Access to logs follows least privilege and data protection controls.

Log retention period: Log retention periods are configurable and agreed with the buyer, subject to the underlying service capabilities.

6.7 Personnel security

Personnel screening: Lean Tree will perform staff screening which conforms to BS7858:2019

Government security clearance: Lean Tree are willing to obtain clearance for relevant individuals up to Developed Vetting (DV).

Staff access restriction: Staff access is restricted to named individuals who require access to deliver the service. Subcontractor access, where used, is controlled and approved at call-off.

6.8 Security incident management

Security incident response process: Lean Tree as an organisation follows a documented security incident response process covering triage, containment, eradication, recovery, and post-incident review.

Buyer notifications: Notification and reporting timescales are agreed at call-off based on the buyer's incident-management process and reporting needs.

Post-incident review: Post-incident reviews capture lessons learned and corrective actions, with actions tracked to closure where applicable.

6.9 Data sanitisation and disposal

Secure disposal approach: Buyer information held by Lean Tree is securely deleted/disposed of in line with the agreed retention schedule.

Deletion confirmation: Deletion confirmation is provided on request and follows the timelines and evidence approach agreed at call-off.

7. Service constraints and assumptions

Assumptions: Delivery is performed within buyer-controlled tenancy/accounts and buyer-approved tooling, unless explicitly agreed otherwise at call-off.

Constraints: Requires outbound HTTPS access from buyer networks to Port. Data ingestion uses push-based methods; inbound connectivity to buyer environments is not required for ingestion. For customers with strict network controls, on-premises Ocean integrations can be deployed in the buyer environment so data can be processed locally and only required results sent to Port. Onboarding timelines depend on integration complexity and buyer readiness; mobilisation is agreed at call-off.

8. Pricing model summary

Charging basis: Pricing is confirmed at call-off based on the selected SaaS subscription and any agreed support services. Third-party licence costs are governed by the buyer's contract with the vendor unless Lean Tree is explicitly acting as a reseller.

Minimum term and payment options: Subscription terms and payment options are governed by the SaaS vendor commercial model and confirmed at call-off.

What is included and what is chargeable: Included items, add-ons, and any additional support services are confirmed at call-off and reflected in the pricing schedule.

9. Quality and service management

Quality management: Lean Tree is implementing ISO 9001 (planned audit April 2026). Lean Tree does not have ISO 9001 certification at this time.

Service management: Lean Tree holds an Information Technology Infrastructure Library (ITIL) Maturity Level 2 certification. Lean Tree does not have ISO/IEC 20000-1 certification.

Information security: Lean Tree holds IASME Cyber Essentials and IASME Cyber Assurance. Lean Tree is implementing ISO 27001 (planned audit April 2026) and does not claim ISO 27001 certification at this time.

Assurance mechanisms: Assurance is provided through peer review, agreed quality gates, and evidence-led deliverables (assurance hooks), aligned to the buyer's governance.

Continuous improvement: Continuous improvement is delivered through retrospectives and service reviews, with actions tracked and agreed at call-off.

10. Exit, offboarding, and data portability

Offboarding steps and timescales: End-of-contract includes: agreement of a termination date; data export window; account and integration decommissioning; administrative confirmation of closure; and data deletion in line with Port (port.io) retention and deletion policy. The supplier coordinates the process and provides a checklist to the buyer.

Data export options: Primary export mechanism is via REST API (JavaScript Object Notation (JSON) over HTTPS). Any additional file-based exports (e.g., Comma-Separated Values (CSV)) are object/integration specific and should be confirmed against the configured data sources and capabilities at the time of offboarding.

Data return/deletion: The buyer can export service catalogue metadata, templates, configuration, and audit information where available. Export methods may include API access and file-based exports. Data extracted and the available export mechanisms are confirmed with Port (port.io) as part of onboarding and documented for the buyer.

11. Dependencies

Buyer-owned subscriptions/accounts: Buyer provides required SaaS subscriptions and any associated accounts, unless Lean Tree is explicitly acting as reseller at call-off.

Identity, networking, and security dependencies: Dependencies (identity provider, network egress, security approvals) are confirmed at call-off and align to buyer standards.

Third-party vendors: Internal Developer Platform SaaS (Port.io) vendor and any configured integrations, as agreed at call-off.

12. How buyers engage and order

Buyers can directly award a Call-Off Contract via G-Cloud in line with the Call-Off Procedure.

Ordering steps:
1) Call-off and integration scope: confirm intended use cases, in-scope integrations, environments, roles and success measures.
2) Tenant and identity readiness: confirm tenant provisioning approach, SSO/identity prerequisites, and admin access.
3) Catalogue and structure design: define domains, service catalogue structure, ownership model and naming standards.
4) Golden paths and templates: implement initial golden paths, scaffolds and self-service actions aligned to standards.
5) Policy and scorecards: configure scorecards, checks and guardrails to drive

consistent delivery behaviour.
6) Toolchain integration: connect CI/CD, Infrastructure as Code (IaC), ticketing and other agreed systems; validate end-to-end workflows.
7) Pilot and iterate: onboard a pilot team, capture feedback, refine templates and governance.
8) Enablement and handover: deliver onboarding materials, operating model, support routes and a scaling backlog.

Implementation timescales: Implementation timescales depend on integration complexity and buyer readiness and are confirmed at call-off.