Klyra Shield

Service Definition Document

Prepared by:	**OfficeLabs Ltd** Queensgate House 48 Queen Street Exeter, EX4 3SR +44 (0)1392 240365
Version:	Issued 1
Last revised:	10/01/2026
Version History:	1

1. SERVICE OVERVIEW

Klyra Shield is a cloud-delivered AI protection service designed to prevent the disclosure of sensitive information when users interact with cloud-based artificial intelligence tools.

The service operates as a browser extension that inspects AI prompts in real time before they are transmitted to third-party AI providers. Where sensitive information is detected, the service automatically blocks the prompt and notifies the user, reducing the risk of data leakage and non-compliant AI usage.

Klyra Shield is typically used by organisations adopting cloud AI tools such as conversational AI and productivity assistants, where there is a requirement to maintain control over sensitive data and demonstrate responsible AI use. The service can be used independently or alongside broader information governance, security, and assurance services delivered under separate engagements.

2. PRODUCT CAPABILITIES

The service provides the following core capabilities:

- Real-time inspection of AI prompts prior to transmission
- Detection of sensitive information including personal, financial, and confidential data
- Automatic blocking of prompts that breach defined policies
- Configurable detection rules, including organisation-specific patterns
- User notifications explaining why content was blocked
- Centralised administrative dashboard for AI usage visibility
- Audit logging and reporting to support compliance and assurance

The service focuses on preventive control and visibility of AI usage, rather than post-incident monitoring.

3. DEPLOYMENT AND OPERATION

Klyra Shield is delivered as a SaaS service supported by a managed browser extension deployed to end-user devices.

Customers access administrative functionality via a secure web-based dashboard. No on-premises infrastructure is required. Prompt inspection occurs locally within the browser environment, with policy enforcement applied before any data is transmitted externally.

The service leverages cloud infrastructure for administration, reporting, and policy management.

4. CONFIGURATION AND CUSTOMISATION

The service is configured through administrative settings rather than bespoke development.

Customers can configure detection rules, policy thresholds, user groups, alert behaviour, and reporting views within defined parameters. Organisation-specific patterns can be defined to reflect internal terminology or risk concerns. The core platform is not custom-built per customer, and no custom code is required for standard operation.

This configuration approach supports consistent enforcement of AI usage policies across the organisation.

5. ONBOARDING AND USE

Customers typically begin by configuring administrative access and defining AI usage policies, followed by deployment of the browser extension to users.

Onboarding focuses on validating policy behaviour, confirming prompt inspection outcomes, and familiarising administrators with reporting and audit features. Initial deployment can typically be completed quickly, subject to browser management arrangements and organisational readiness.

Optional onboarding assistance and advisory services are available under separate Cloud Support service listings.

6. SUPPORT AND ASSURANCE MODEL

Standard SaaS support is included with the service subscription and covers incident logging, investigation, and resolution of software-related issues.

Enhanced support options, onboarding assistance, advisory services, and ongoing managed support are available separately under applicable Cloud Support service listings. These services are not included as part of the standard SaaS product.

7. SECURITY, AVAILABILITY, AND COMPLIANCE

The service is designed to support secure and compliant use of cloud-based AI tools. Prompt inspection and policy enforcement occur locally within the browser environment, reducing the risk of sensitive data being transmitted externally.

Availability and resilience are provided through the underlying cloud hosting platform supporting the administrative and reporting components. No formal uptime service level agreement is included as part of the standard service.

Detailed security and compliance controls are described in the Digital Marketplace listing and supporting assurance documentation.

8. DATA, EXIT AND COMMERCIAL NOTES

Customers retain ownership of their data at all times. Usage data and audit logs can be exported using supported formats prior to contract termination.

At the end of the contract, access to the service is withdrawn in line with agreed notice periods, and browser extensions are removed using standard device management processes. No customer data is retained beyond defined operational backup periods.

Pricing, contract terms, and any trial or assessment arrangements are defined in the Digital Marketplace listing and associated commercial documentation.

9. RELATIONSHIP TO OTHER SERVICES

Klyra Shield is commonly used alongside information governance, security assurance, and AI adoption support services. These services are optional and are delivered under separate contracts or service listings where required.