G-Cloud 15 Service Definition Document
Service Type: Lot 2b - Software as a Service (SaaS)
Service Name: Zone Standard - Minvera

Service overview

Zone Standard – Minerva is a secure, cloud-based NHS risk, incident and compliance management platform that supports the end-to-end management of risks, incidents, complaints, requests for information (RFI) and claims. Zone Standard – Minerva is an approved supplier of a Local Risk Management System (LRMS) approved by NHS England, supporting LFPSE v6 reporting and PSIRF-aligned workflows to enable consistent triage, investigation, actions, learning and governance.

Minerva provides configurable modules, standardised data capture and role-based workflows to support trust-wide adoption. Role-based access controls and comprehensive audit trails support accountability, defensible decision-making and consistent operational governance.

Service scope

Minerva provides configurable workflows and registers to support governance processes across clinical and non-clinical teams. Typical capabilities include structured intake, triage, tasking, review and approval, action tracking, learning capture, and reporting. The service supports operational use at team level as well as executive oversight through dashboards and scheduled reporting.

Minerva is delivered as a browser-based SaaS service. Configuration is performed within defined parameters to maintain a standardised, supportable platform while enabling local operating models, governance routes, roles and reporting structures to be reflected.

LFPSE v6 and PSIRF workflow support

Minerva supports LFPSE v6-aligned data capture and reporting, enabling the consistent collection of required data items and the production of reports aligned to national and local oversight needs. PSIRF-aligned workflow support enables structured triage and proportionate response pathways, investigation management where required, governance review and sign-off, and the tracking of actions and learning to closure.

Workflows can be configured to reflect local governance structures, escalation routes and review groups, supporting consistent application across divisions, sites and services.

Clinical safety and governance

Minerva supports learning-focused governance and operational workflows, including structured triage, investigation management, action tracking and evidential reporting. Where deployed in NHS environments, implementation and ongoing service use are managed under appropriate organisational governance, information governance and change control processes. Configuration is agreed during onboarding to reflect local operating models, roles and responsibilities, ensuring consistent and controlled adoption.

Reporting & Alerts

Minerva provides operational, management and executive reporting to support oversight of risks, incidents, investigations, actions, complaints, RFIs and claims. Role-based dashboards present key measures such as volumes, status, timeliness, overdue items, themes and trends. Reporting can be configured to reflect organisational structures (for example, divisions, directorates, services and sites) and to support governance forums through exports and scheduled reporting packs where required.

Minerva supports alerting to drive timely action and escalation. Notifications can be configured around workflow events and thresholds such as new submissions, assignment changes, requests for review or approval, approaching due dates, overdue actions, and escalation triggers aligned to local governance processes. Alerts are targeted to relevant users and roles to support timely follow-up and auditable accountability.

Onboarding and implementation

Onboarding is delivered through a structured implementation approach, typically including discovery and configuration workshops, environment setup, role and permission design, workflow configuration, user acceptance testing support and training for administrators and end users. Implementation can be delivered as phased rollout or ‘trust-wide go-live’ depending on customer preference and readiness.

Where agreed, onboarding can include data migration and integration activities, subject to technical feasibility, availability and quality of source data, and customer-side approvals and dependencies.

Service management and support

Minerva is supported through a support desk operating defined processes for incident management, service requests and escalation. Post go-live support includes troubleshooting, platform guidance, configuration queries within agreed scope, and service communications including release notes and update notifications. Regular service review arrangements can be provided where contracted.

Optional services may include enhanced support hours, additional training, reporting support, and change requests or additional configuration delivered through controlled change processes.

Service levels

Minerva is operated with defined service levels covering availability, incident response and support performance. Incidents are triaged and managed based on severity and impact, with appropriate escalation and communications. Monitoring and operational processes are used to maintain platform reliability and performance. Specific availability targets, support hours and response targets are defined in the service schedule and contract.

Maintenance management

For unplanned service incidents, Zone Standard confirms the incident, initiates investigation and provides updates through agreed communication channels. Updates include impact assessment, progress, mitigations or workarounds where available, and confirmation when service is restored. Where appropriate, a post-incident summary can be provided covering cause, impact and corrective actions.

Planned maintenance is scheduled to minimise disruption and communicated in advance where practicable. Customers are informed of relevant release activity and any required customer actions (for example, validation of integrations following changes) through agreed service communications.

Technical requirements

Minerva is accessed via a modern web browser and requires a stable internet connection. Users require valid authentication credentials and permissions granted through role-based access controls. No specialist client software installation is required for standard use.

Customers are responsible for maintaining appropriate endpoint security, supported browser versions and network controls in line with their organisational policies. Where integrations are implemented, customers provide access to relevant technical contacts, interface specifications and third-party coordination as required.

Hosting and data residency

Minerva is delivered as a cloud-hosted SaaS service. Hosting location and data residency commitments are defined contractually. Hosting is operated with security and resilience controls appropriate for UK public sector use, and any customer-specific hosting or residency requirements are confirmed during procurement and contract.

Data backup, restore and disaster recovery

Minerva operates with documented backup, restore and disaster recovery arrangements to support service resilience and continuity. Platform data is backed up routinely in line with defined operational procedures, with backups protected to maintain confidentiality and integrity. Restore processes are maintained and periodically tested to provide assurance that data can be recovered following accidental deletion, data corruption or a service incident.

A disaster recovery plan is maintained to support continuity in the event of a major platform outage. Recovery responsibilities, processes and operational runbooks are defined and exercised periodically. Where customer-specific recovery objectives are required (for example, recovery time and recovery point targets), these are defined contractually.

Security

Zone Standard maintains an ISO/IEC 27001-certified information security management system (ISMS) and an ISO 9001-certified quality management system to support controlled delivery and continual improvement. Zone Standard holds Cyber Essentials Plus certification, and Minerva is subject to annual penetration testing, with findings managed through controlled remediation and change processes.

Minerva applies encryption to protect customer data in transit and at rest. Data in transit is protected using industry-standard TLS. Data at rest is protected using managed encryption controls. Access to the service is controlled using role-based access control (RBAC) to restrict functions and data to authorised users. Audit logging records key administrative and user activities to support accountability, compliance monitoring and investigation where required. Secure development and operational practices are applied across the service lifecycle, including code review, vulnerability scanning, dependency management and controlled release pipeline.

Service constraints

Minerva is delivered as a standardised SaaS service with configuration available within defined parameters to maintain security, performance and upgradeability. Some changes may require scheduled release activity and may be delivered through change control.

Minerva requires reliable internet access and a supported modern web browser. Service performance is dependent on customer endpoint configuration, local network conditions and the performance/availability of any connected third-party systems used for integrations.

Offboarding and access to data on exit

Customers retain ownership and control of their data throughout service use and offboarding. On exit, Minerva supports export of customer data in agreed formats suitable for retention, audit and transition to another system. Following confirmation of successful extraction, customer access is removed and remaining data is managed in accordance with contractual terms, retention requirements and secure deletion processes.

Summary

Zone Standard – Minerva is a secure, cloud-based NHS risk, incident and compliance management platform and an NHS England-approved Local Risk Management System (LRMS) supplier. It supports the end-to-end management of risks, incidents, complaints, requests for information (RFI) and claims, with LFPSE v6 reporting and PSIRF-aligned workflows to enable consistent triage, investigation, action tracking, learning capture and governance oversight.

The service is delivered as a browser-based SaaS platform with onboarding, optional migration and integration services (subject to scope), defined support arrangements, and resilience controls including backup, restore and disaster recovery. Security assurance is supported through ISO 27001, ISO 9001, Cyber Essentials Plus and annual penetration testing, alongside encryption, RBAC and audit logging.