

Service Definition — Recruitment Applicant Tracking System (ATS)

G-Cloud Lot: 2b — Software as a Service (SaaS)

Service type: Public cloud SaaS

Service name: Recruitment Applicant Tracking System

1. Service overview (what the service is)

Recruitment Applicant Tracking System is a cloud-based Applicant Tracking System (ATS) that supports the full recruitment lifecycle, including vacancies, applications, shortlisting, interviews, offers, and reporting. The service is delivered as SaaS and accessed through a secure web browser, with no local installation required.

The platform is designed for administrators, recruiters, hiring managers, and candidates, enabling structured workflows, consistent processes, and clear auditability of recruitment activity.

2. Service features and benefits

Features

- Configurable vacancy workflows with multi-stage recruitment processes
- Branded candidate portals for a consistent applicant experience
- Structured application forms with custom fields and validation controls
- Automated screening and shortlisting tools
- Interview and event scheduling with calendar integration
- Role-based access controls for secure user permissions
- Agency management tools for external recruiter submissions
- Recruitment dashboards and EDI reporting for compliance analysis
- Secure cloud SaaS delivery with managed updates and monitoring

Benefits

- Reduce time-to-hire through streamlined recruitment processes
- Improve candidate experience through clear communication and user-friendly portals
- Increase recruitment consistency using standardised workflows and templates
- Enhance compliance through auditable hiring steps and EDI reporting
- Support high-volume hiring with efficient screening and filtering
- Reduce administrative effort through automation and templates
- Improve visibility for hiring managers via real-time dashboards and statuses
- Strengthen data security using controlled access and encrypted storage
- Enable data-driven decisions through recruitment and diversity analytics
- Simplify IT operations through a fully managed SaaS service

3. Service scope and constraints

Deployment model: Public cloud (SaaS)

Multi-cloud support: No

Service constraints

The service may experience brief planned maintenance during agreed windows and requires supported web browsers and internet connectivity. Customisation is limited to configuration options available within the standard SaaS platform.

Customisation

Buyers can customise workflows, forms, branding, email templates, vacancy templates, and user permissions through the admin interface. Customisation is configuration-based and does not require code changes. Only authorised administrators with appropriate permissions can make changes.

4. User access, interface, and accessibility

Service interface

The service is accessed through a secure, role-based web interface. Navigation, workflows, and forms adapt to user permissions, providing streamlined access to recruitment tasks and candidate data.

Supported browsers

- Microsoft Edge
- Firefox
- Chrome

Accessibility

The service interface supports WCAG 2.2 AA. Accessibility testing includes screen reader support, and validation using common assistive tools.

Online ticketing support accessibility also supports WCAG 2.2 AA.

5. Service levels (availability, resilience, and support)

Availability and resilience

The service provides 99.9% availability via elastic containers and an AWS multi-zone layout. Resource usage is monitored and the platform scales to handle increased demand. Each customer operates in a multi-tenant system with separate databases and capacity controls to prevent one organisation's activity from impacting another.

Outage communications

Service outage reporting and updates are provided through dashboard updates and email notifications.

Support channels and hours

Support is available via:

- Email / online ticketing: Yes
- Phone support: Yes (09:00–17:00 UK time, Monday to Friday)
- Web chat: No
- Onsite support: No

Support queries are responded to within the standard SLA, typically during business hours. Higher-priority issues receive faster initial response. Weekend and bank holiday responses occur the next working day unless otherwise agreed.

Support includes priority-based response targets for incidents and service requests. An assigned Account Manager provides regular reviews and acts as the main escalation point. Enhanced support (such as extended hours or dedicated technical assistance) may be provided as a chargeable add-on. Support can be made available to third parties where required.

6. Onboarding and offboarding

Onboarding

Structured onboarding is provided, including configuration support, online training sessions, and access to user and administrator documentation. A dedicated implementation lead supports setup, testing, and go-live to help buyers adopt the service quickly.

Documentation

Service documentation is available in:

- PDF
- Online helpdesk
- In-app product support
- Documentation is designed to support WCAG 2.2 AA.

Offboarding and end-of-contract process

At contract end, buyers can export their data and access the service until the agreed termination date. After closure, user access is removed and data is securely deleted or anonymised in line with GDPR and retention policies.

Standard offboarding (data export via built-in tools and account closure) is included in the contract price. Large bespoke exports, extended access periods, or migration support may incur additional costs.

7. Data import/export and analytics

Data export

Buyers can export data through built-in reporting and export tools. Bulk extracts can also be provided through secure transfer methods before contract closure. Data extraction processes follow GDPR requirements for secure handling and lawful transfer of personal data.

Export formats supported:

- CSV
- PDF

Service metrics and reporting

The service provides metrics including vacancy activity, application volumes, stage progression, time-to-hire, source performance, and EDI reporting. Administrators and hiring managers can access real-time dashboards and export reports for analysis.

8. Hosting and data residency

Hosting location

Data storage and processing takes place in the United Kingdom. Buyers do not control data storage and processing locations.

Data centre standards

The hosting environment complies with recognised security standards, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402.

9. Security (technical and operational)

Data protection in transit

Data is protected between buyer and supplier networks using TLS 1.2 or above, and within the supplier network using TLS 1.2+ and/or IPsec/TLS VPN gateway protections.

Data protection at rest

Data at rest is protected through physical access control (aligned to recognised cloud standards) and encryption of physical media.

Penetration testing

Penetration testing is performed at least once per year by an NCSC approved service provider.

Vulnerability and change management

Changes are tracked in Jira and monitored for vulnerability and license issues using Snyk.

Vulnerability management includes assessment of surface attack area, probability, and impact. Zero-day issues are resolved the same day. Critical and high severity issues are remediated before release to production. Threat intelligence sources include AWS and Snyk.

Monitoring and incident management

Protective monitoring uses AWS logging and alerting infrastructure, with real-time review and remediation. Incident management procedures are in place to address availability, component, and security incidents, supported by a defined escalation tree. Major incidents are escalated to the CTO and tracked in Jira.

Identity and authentication

User authentication is required and supports:

- Multi-Factor Authentication (MFA)
- Username and password

All management interfaces are protected behind a Microsoft identity provider with 2FA enforced. Access restrictions are tested at least once per year.

Audit logging

Buyers have access to real-time audit information for user actions. Audit data is stored for at least 12 months. Supplier activity audit information can be provided via support request. Supplier audit data is stored for at least 12 months. System logs are stored for at least 12 months.

Data sanitisation and disposal

Data sanitisation is supported via cryptographic erasure and data erasure processes ensuring deleted data cannot be directly accessed. Equipment disposal is performed using a third-party destruction service.

10. Technical requirements

Buyers require:

- Modern browser (Chrome, Edge, Firefox) with JavaScript enabled
- Stable internet connection over HTTPS (port 443)
- Email access for notifications and system communications
- Cookies enabled for secure session management
- Desktop or laptop device with updated operating system
- Pop-up permissions enabled for certain functions
- PDF viewer for exported reports and documents
- Admin access to organisation email settings (as required)
- Optional SSO requires a compatible identity provider
- No local installation or VPN required