JobAdder

2026

Security and Trust FAQs

Building trust through transparency

Company summary

Name of software vendor	JobAdder Operations Pty Ltd
ABN	39 167 597 953
Name of software product	JobAdder
Jobadder Compliance Certifications	ISO 27001:2022
Primary address	Level 28, 121 Castlereagh Street Sydney NSW 2000
Security officer	Rohan Blake - vCISO
Contact email	Raise a ticket - https://support.jobadder.com/hc/en-us
URL of application or service	https://rms.jobadder.com
Marketing Site	https://jobadder.com
Operating Countries	Australia, New Zealand, UK, USA, Canada
Hosting Provider	Amazon Web Services - https:// www.aws.com
Privacy policy	https://jobadder.com/privacy
Terms of Use	https://jobadder.com/terms
# of Employees	~210
# of Customers	~5050

Security and Trust FAQs

Introduction

Choosing a recruitment platform is about trust, and JobAdder is engineered to be your reliable partner. We offer a high-availability platform built on AWS; but we don't just provide software; we provide world-class, human-led support that follows the sun.

Our global team is available 24/6 across Australia, the UK, and the US.

Data and Privacy

Where are JobAdder's data centres located?

JobAdder is hosted on Amazon Web Services (AWS). Production/live data is stored in the AWS region that aligns with the customer's location.

AWS Regions:

- Asia Pacific (Sydney)
- US West (Oregon)
- Canada (Central)
- EU (Ireland)

Does JobAdder have documentation that describes scenarios in which data may be moved from one physical location to another?

Production data remains within the customer's selected AWS region and does not leave that region except where a customer explicitly requests a data export, such as when terminating their JobAdder's subscription. This is outlined in the JobAdder Terms of Use.

How does JobAdder protect data-at-rest?

- All data is encrypted at rest using AES256.
- Database data is stored on AES256 encrypted EC2 volumes.
- S3 buckets are AES256 encrypted using S3-managed keys.

How does JobAdder protect data-in-transit?

HTTPS using TLS 1.3 with approved secure ciphers is required for all web applications.

How does JobAdder store payment / credit card information?

JobAdder does not store any credit card information. All subscription and payment processing is handled by Stripe, which is PCI DSS compliant. Please see: https://docs.stripe.com/security. For payment methods such as Direct Debit, Jobadder uses GoCardless, with custom payment pages integrated for collecting payment details.

Security and Trust FAQs

Does JobAdder provide tenants with separate environments for production and test processes?

Yes. Jobadder provides separate pre-production environments for integration and testing, and these environments do not contain any production data. If a customer requires production data for testing purposes, a separate UAT environment can be created per customer.

How does JobAdder ensure production data is not replicated or used in non-production environments?

Personally Identifiable Information (PII) does not exist in non-production environments. Production and Non-Production environments are located in separate data centres on separate networks.

Identity and Access Management

How do customers authenticate and login to JobAdder's platform?

JobAdder provides two options for authentication to the platform: JobAdder local accounts, or SSO using customers' own IdP (via OIDC or SAML 2.0).

For local accounts:

- Minimum 15-character password
- Blocklist for common words
- Password history checks (cannot reuse the last five passwords)
- Account lockout after five unsuccessful attempts (5-minute lock)

For MFA & Passkeys:

- OTP-based MFA is available for all users including local accounts and can be enforced by the customer's account administration.
- Passkeys are available for all users to login to Jobadder using device-based authentication (e.g. fingerprint, face or device PIN). Passkeys provide a phishing-resistant alternative to passwords and can be used as a faster, more secure way to log in.

For SSO:

- Can be implemented using either OIDC and SAML 2.0
- Customers can define their own password/authentication and session requirement

How is authorisation and Role-Based Access control implemented in the JobAdder application for Customers?

Role-based access control is available with two primary user types: *Admin* and *Standard* - with support for granular and function specific permissions.

These permissions can be assigned access to specific actions such as:

1. Add contact as hiring manager
2. Approve placement

Security and Trust FAQs

3. Manage placement credits
4. Delete records
5. Delete and Edit notes
6. Merge candidates
7. Export spreadsheets
8. Edit interview evaluation
9. Grant API access to integration partners
10. Manage financial custom fields.

How do JobAdder staff authenticate?

JobAdder staff must use a minimum 15 character password and MFA is mandatory for all systems used by JobAdder infrastructure administrators.

What processes does JobAdder have in place to manage identity and access for staff?

Jobadder manages staff access to internal and third-party systems using our Corporate SSO Identity Management platform. Processes include:

- Multifactor authentication (MFA) required for employees accessing production systems
- Information Management systems (e.g. application servers, firewalls, APIs) have logging and monitoring enabled
- The detail and levels of access of personnel who have access to IT infrastructure changes are managed and stored with individual accounts
- Access to logging and monitoring reporting is restricted to appropriate personnel
- Password changes are forced upon first logon to systems
- All access approvals and evidence are recorded for audits as per ISO 27001 requirements.

Is privileged access across Information Systems reviewed on a periodic basis?

Yes, Privileged access reviews are performed on a quarterly basis.

Network and Infrastructure Security

How secure are JobAdder's data centres?

JobAdder's data centers are provided by AWS, which maintains ISO 27001 and ISO 9001 certifications. A current list of its compliance programs and standards can be found here.

Physical access to AWS data centres is restricted to authorised AWS personnel only.

AWS also provides SLAs of 99.9% or higher for core services such as Amazon Simple Storage Service ("S3") and messaging services (such as Amazon EventBridge, Simple Notification Service ("SNS") + Simple Queue Service ("SQS").

Security and Trust FAQs

What measures does JobAdder have in place with regard to Infrastructure Security?

JobAdder implements multiple infrastructure security measures, including:

- Synchronised time-service protocol (NTP) to ensure all systems have a common time reference
- Regular reviews of servers and system capacity to ensure current and anticipated capacity can meet customer needs
- Files-upload validation against a whitelist of allowed file types/extensions.
- Automated encryption key rotation and secrets management via AWS
- Continuous scanning and monitoring of external facing assets using enterprise tooling

What Network Security controls are in place?

JobAdder uses a layered network security model, including:

- Cloudflare WAF for web application firewall and DDOS mitigations.
- AWS Network Load Balancer, restricts access to only required ports/services.
- AWS Security groups are utilised for network segmentation on a least access model
- Hardened operating system baselines on application servers to provide only necessary ports, protocols, services and applications as part of the baseline standard build.

What Operating System controls are in place?

JobAdder runs web and application servers on hardened Windows Server and Linux AMIs. Controls include:

- Prompt installation of Windows Updates, hotfixes and service packs
- Network-level port blocking
- Disabling of unnecessary services
- Anti-malware and Enhanced Detection Response (EDR) is deployed on all infrastructure and continuously updated
- Log forwarding to New Relic for monitoring and alerting.

What anti-malware and endpoint detection controls are in place?

All endpoints, including laptops and servers, have anti-malware and Endpoint Detection and Response (EDR) software is installed and actively monitored.

Our enterprise EDR platform analyses files and programs for behaviour patterns to identify malware, indicators of attack, and suspicious activities.

What logging, monitoring and threat detection controls are in place?

JobAdder uses next-generation SIEM platform that ingests logs from key sources including identity systems, cloud security services and endpoint protection tools across laptops and servers.

Security and Trust FAQs

Additional monitoring and detection controls include:

- NextGen AV and EDR with proactive threat hunting
- New Relic which ingest AWS infrastructure, WAF and application logs to generate alerts for unusual activity
- AWS GuardDuty for anomaly and threat detection across AWS services
- AssetNote for continuous external attack-surface monitoring

Software Development Lifecycle (SDLC) & Change Management

How does JobAdder detect security defects in code prior to production?

JobAdder applies secure development and testing practices, including:

- Architecture Design Reviews (ADR) are performed prior to the development of new significant features to assess both function and security.
- JobAdder uses a Pull-Request model for software development changes requiring at least two separate people to approve code before it reaches production.
- There are both automated and manual checks for security vulnerabilities and issues are addressed prior to deployment.
- JobAdder uses automated static code analysis (SAST) and Software Composition Analysis (SCA) to review source code for production applications.
- Dynamic Application Security Testing (DAST) Web Application Scanning is performed across Jobadder applications checking for OWASP Top 10 vulnerabilities.
- JobAdder has controls and standards in place to ensure standards of quality are being met for software development. These include, but are not limited to: Authentication, Authorisation, Input/Output validation, Session Management, Exception Management, Logging, Encryption & Cryptography.
- When issues are reported in production, there is a procedure in place to remedy these as soon as they are identified.

What is JobAdder's Change Management process?

JobAdder has a documented Change Management policy and process for managing changes to its information processing facilities and production systems.

Changes are managed through a risk-based, engineering-led process aligned with continuous delivery practices, with oversight provided by engineering leadership and peer reviews.

Changes are classified as Minor, Major, or Emergency based on risk, customer impact, and complexity, determining the level of review and documentation required.

Implementation involves approved engineering practices, validation in non-production environments, and the use of automated CI/CD pipelines, with rollback mechanisms in place.

Security and Trust FAQs

- Changes are implemented using approved engineering and deployment practices, including Infrastructure as Code (IaC) where applicable.
- Changes are validated in appropriate non-production environments or through approved testing mechanisms prior to release.
- Automated CI/CD pipelines are used for regular deployments
- Changes may be deployed incrementally, by environment, region, or feature flag.
- Rollback or mitigation mechanisms must be available prior to release.

Technical Architecture and High Availability

What is JobAdder's technical architecture for high availability?

JobAdder is a multi-tenanted SAAS provider, hosted on AWS, where customers' data is logically separated to ensure no cross contamination takes place. Account segregation is controlled by programmatic access controls.

Our multi-cluster, multi-tenanted environment is designed with key controls to ensure high availability and prevent a single downtime event from impacting all clients:

- Architectural Isolation: We have 11 distinct, multi-tenanted instances/clusters spread across 4 global geographic regions. This provides physical and logical fault isolation, ensuring a failure is contained to a minimal blast radius, protecting the service for the vast majority of our global client base.
- Data and Recovery Objectives are implemented to meet the business continuity targets:
  - RPO (Recovery Point Objective): 15 minutes (Maximum acceptable data loss).
  - RTO (Recovery Time Objective): 2 hours (Maximum acceptable time to restore service).
- Deployment Safety: JobAdder employs staged rollouts as a primary control for deployment safety. By utilizing automated CI/CD pipelines and feature flags, we release updates to small, isolated clusters and specific geographic regions (e.g., CA, US) before a global rollout. This 'canary' approach allows our team to monitor system health in real-time, effectively containing any potential issues to a minimal blast radius and ensuring that 100% of critical features remain available to the vast majority of our users during any update.

How is JobAdder's application architected for resilience and availability?

(1) CloudFlare WAF
Cloudflare WAF provides web application firewall and DDOS mitigation services.

(2) Elastic Load Balancer
AWS Elastic Load Balancers distribute traffic across redundant servers hosted across three availability zones within the AWS selected region, ensuring continuity if one zone becomes unavailable.

(3) Auto Scaling Groups
Auto Scaling Groups (ASGs) automatically replaces unhealthy instances and consistent application capacity.

Security and Trust FAQs

(4) Document Storage
Documents (resumes, cover letters, etc) uploaded are stored in encrypted S3 buckets which have a 99.999999999% (11 9's) of durability.

(5) Database
Database data is stored on encrypted EC2 volumes and on Amazon RDS. Data is mirrored asynchronously to a redundant server. Backups are managed and securely stored in AWS.

(6) Backups
Backups are managed and securely stored in AWS. The SQL database is backed up according to the following schedule; weekly full backup, nightly differential backup & 15min log backups.

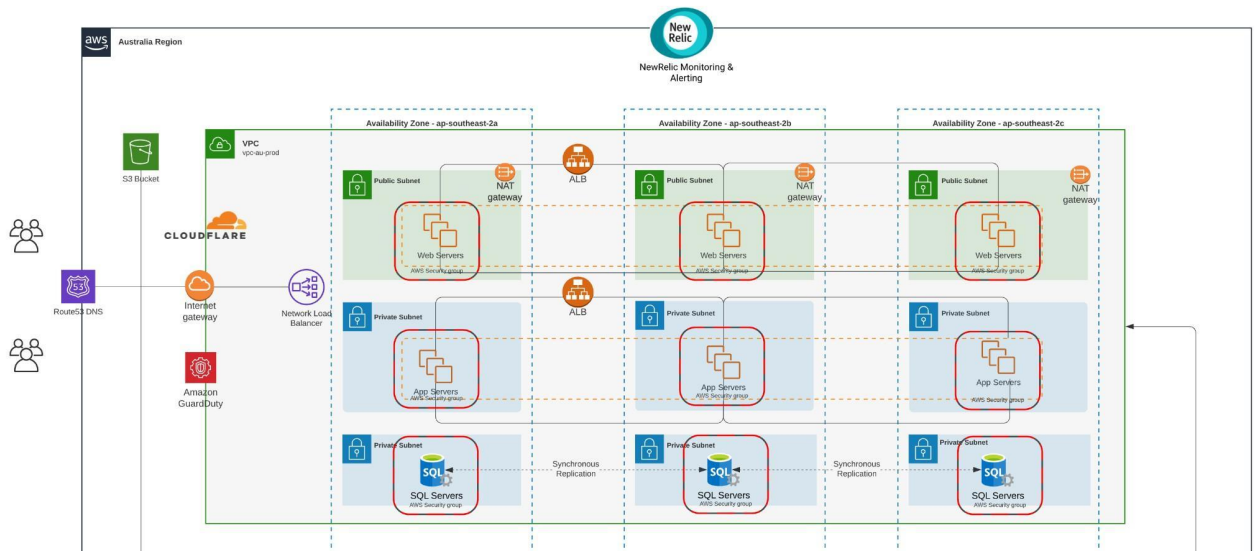
(7) Recovery objectives
RTO is 2 hours. RPO is 15 minutes, the maximum duration of a DB transaction log backup.

(8) Monitoring and metrics
Cloudwatch and New Relic are used to monitor and provide application and server metrics.

JobAdder is committed to maintaining industry best practices by leveraging a high-availability architecture built on AWS. Our operations are aligned with global standards, like ISO 27001:2022 to ensure that its high-availability architecture remains secure and reliable.

The underlying AWS services used by JobAdder are independently certified for ISO 27001, as well as SOC 1 and SOC 2, which strengthens the overall resilience of the infrastructure.

To achieve engineering excellence, JobAdder aligns its practices with the DORA (DevOps Research and Assessment) framework—the industry standard for measuring software delivery performance.



Security and Trust FAQs

Does JobAdder track performance metrics and benchmarks?

Yes, JobAdder tracks and reports monthly on top-level metrics including availability, MTTR (Mean Time to Recover), change failure rate, and deployment frequency. In 2025, the Change Failure Rate was 1.9%.

The following results are monthly average across 2025

Uptime (%)	99.99
Availability^ (%)	99.86 (Internal target of 99.9)
Mean Time to Recover (MTTR)	57 mins
Change Failure Rate (%)	1.9

^Availability is not merely uptime, rather it is the full functioning of 100% of a defined set of critical features - the system is considered available if and only if all those features are working. JobAdder has an internal target of 99.9 for availability.

Service and Support Agreements

JobAdder operates on a high-availability infrastructure (AWS) with a guaranteed uptime of 99%. Regarding support, JobAdder provides global coverage 24 hours a day, 6 days a week. You can also see our standard Service Level Agreement (SLA) here.

What is the uptime guarantee?

- JobAdder provides a 99% uptime guarantee as part of our Standard SLA
- Calculation: This is calculated as the total minutes in the month minus the total minutes of downtime (excluding scheduled maintenance)
- Uptime on average each quarter is 99.99

What support services are available?

JobAdder provides the following Global Support Services:

- Live-Support: Connect with a live person 24 hours a day, 6 days a week. *excludes Lite package
- Multi-Channel Access: Support via In-app Live Chat, Email, and Phone.
- Global Presence: Support hubs in Australia, UK, and the US to follow the sun.
- Status Updates: JobAdder maintains a publicly available status page, which includes system availability detail, schedule maintenance, service incident history, and the ability for customers to subscribe to real-time updates.
- 96%+ Customer Satisfaction (CSAT) rating consistently maintained.

Security and Trust FAQs

What are the support Service Level Agreements (SLA)?

JobAdder provides free and unlimited support 24 hours a day 6 days a week, Monday through to Saturday (excluding public holidays or other days notified to you). Support SLAs are documented in our Standard SLA terms, tiered by issue severity.

See Definitions section in the standard SLA for Error Severity descriptions:

Error Severity	Service Level
Critical	Workaround of the problem within 8 business hours from the time of Reporting
Serious	Workaround of the problem within 16 business hours from the time of Reporting
Medium	Workaround of the problem within 5 business days from the time of Reporting

How can customers check the status of the JobAdder platform?

Customers can check real-time availability and performance by visiting https://status.jobadder.com. The status page provides updates to JobAdder's platform or any related services that are experiencing any degradation.

How is Maintenance performed?

Standard maintenance is typically performed during low-traffic windows such as weekends and overnight. There is usually minimal disruption. For significant updates, we provide at least 48 hours advance notice.

Business Continuity & Disaster Recovery

Does JobAdder have a Disaster Recovery (DR) and Business Continuity Plan (BCP)?

Yes. JobAdder has a documented backup and disaster recovery (DR) strategy that is part of its broader Disaster Recovery and Business Continuity framework.

We perform regular full, differential and 15-minute transaction log backups of all production databases to encrypted AWS S3 storage in a separate backup account, with retention governed by our central Data Retention Policy. Backups and restores are regularly tested (including periodic DR/BCP exercises) to meet defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets.

Security and Trust FAQs

Backup Frequency:

- Full Backups: Weekly.
- Differential Backups: Nightly.
- Transaction Log Backups: Every 15 minutes.

RPO (Recovery Point Objective): Because of the 15-minute log backups, the maximum potential data loss in a disaster scenario is 15 minutes of data.

Encryption: All backups are managed within AWS and encrypted at rest using AES-256.

Disaster Recovery testing is performed annually under JobAdder's ISO 27001 Business Continuity and DR program, and the underlying AWS services are independently certified (ISO 27001, SOC 1/SOC 2), strengthening infrastructure resilience.

How often do you perform DR Testing?

Disaster Scenarios are mapped and reviewed on an annual basis. Disaster Recovery testing is completed on an annual basis.

Incident Management

Does JobAdder have an Incident response plan?

Yes, JobAdder maintains a formal information security incident management plan that is implemented and maintained in accordance with ISO/IEC 27001 requirements. The process involves:

1. Containment and collection of evidence relating to the incident
2. Identify potentially affected customers/individuals and evaluate the associated risk
3. Assess whether customer/individual/regulatory notification is required
4. Conduct post incident report with root cause analysis to prevent a repeat.

How does JobAdder manage incidents and outages?

JobAdder uses New Relic and AWS Cloudwatch for observability, monitoring and anomaly detection, which feeds into our alerting framework. We have a team ready 24x7, for response when an alert is triggered. Incidents and outages can also be triggered manually through reports via our Support Team. When an incident is detected, our team immediately responds to ensure the service is restored in the shortest time possible.

During all incidents, we keep our status page online updated with details during outages, and anyone subscribed will also get these updates.

After all incidents, we conduct a post-incident review (PIR), to analyse the root cause of the event and develop a list of immediate actions to make sure we prevent the event from happening again. Each PIR is documented in detail and future learnings are incorporated into long term plans.

Security and Trust FAQs

Vulnerability Management & Audits

Are external audits performed?

Yes. JobAdder undergoes annual independent audits as part of our ISO 27001 certification, performed by Lloyd's Register Quality Assurance (LRQA). In addition, annual penetration testing is performed by CREST-certified, and further testing is performed for significant architectural changes.

How often are penetration tests performed and who performs them?

As part of our ISO 27001 certification, annual penetration testing is performed by CREST - certified tester on JobAdder's platform. Penetration results are available once an NDA has been signed.

AI Governance & Security

What is Adder Intelligence and how does it operate within the JobAdder platform?

Adder Intelligence is JobAdder's AI-assisted features that enhance user workflows within the Jobadder platform.

Where can I find information on AI security and bias?

For more AI security and bias control questions about Adder Intelligence, please visit the FAQ section on this page: https://jobadder.com/ai-recruitment-software/

Governance, Risk & Compliance (GRC)

Does JobAdder Maintain any Security / Compliance Certifications?

JobAdder is certified to ISO 27001:2022. The certification is issued by Lloyd's Register Quality Assurance (LRQA).

Does JobAdder implement Compliance and Risk Management Programs?

Yes. JobAdder is certified to ISO 27001:2022 and operates an associated information security risk management program. This includes ongoing risk identification, assessment, treatment and periodic reviews in alignment with ISO 27001 requirements.

What procedures and policies are in place for changes in staff employment and/or termination?

There are a number of controls in place including:

- All employees are required to accept the confidentiality provisions of the JobAdder employment agreement as a condition of employment
- Onboarding and offboarding tasks for each employee are stored and logged in JobAdder's HRMS, ensuring access provisioning and removal follow defined procedures.

Security and Trust FAQs

Where are JobAdder's development and infrastructure administration teams located?

While core software development and administration is predominantly undertaken in JobAdder's Sydney office. JobAdder also engages a small team of developers in Vietnam. JobAdder has the global infrastructure and processes in place to be able to support developers anywhere.

For core software development projects, JobAdder enjoys a highly collaborative, mission-oriented development team which works closely with other functions in the business.

- JobAdder sees the interaction between Developers, Sales and Customer Success teams as essential.
- Close collaboration between development teams and business teams ensures all teams intimately understand how products are being used, and the experiences customers are having.
- This point of difference plays a huge part in JobAdder's 99% customer satisfaction ratings.
- The Support and Sales functions have teams based in AU, the UK, USA and Canada, however, they do not have direct access to data:
- Support can only view a customer's account with that customer's permission
- Access can be granted for 3 days, 1 week, 2 weeks, 4 weeks or 8 weeks.

Do you have any security Questionnaires / CAIQ already completed?

Yes, you can find JobAdder's v4.03 CAIQ document by clicking here.

General Service Questions

Does JobAdder have an API?

Yes. All available services along with API documentation can be found here: https://developers.jobadder.com/docs.

What platforms/devices can JobAdder be accessed from?

JobAdder is a web-based SaaS application and can be accessed from any device (e.g. Windows, Mac etc) that supports a modern web browser. The platform is designed for browser use and supports the latest versions of all major browsers.

How can customers check the status of the JobAdder platform?

Customers can check real-time availability and performance by visiting https://status.jobadder.com. The status page provides updates to JobAdder's platform or any related services that are experiencing any degradation.

JobAdder

Adding **Joy** to the Job of Recruitment