JobAdder

2026

Security 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

©2024 Copyright JobAdder Operations Pty Ltd. All rights reserved.

Security FAQs

Introduction

JobAdder is a cloud-based recruitment management services system delivered to the end user via a web browser or mobile device. The purpose of this document is to provide an overview of common security questions.

Security FAQs

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)

Production data does not leave its designated geographic boundary. Compute is distributed across multiple AWS availability zones for resilience and high availability. No cross-region data migration occurs unless requested by the customer.

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.

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.

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.

©2024 Copyright JobAdder Operations Pty Ltd. All rights reserved.

Security FAQs

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 SAML2).

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)
- Passkeys are supported, providing a phishing-resistant and user-friendly authentication option that adds an extra layer of protection for customer accounts.

For MFA:

- OTP-based MFA is available for all users and can be enforced by the customer's account administrator.

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:

- Add contact as hiring manager
- Approve placement
- Manage placement credit
- Delete records
- Delete and Edit notes
- Merge candidates
- Export spreadsheets
- Edit interview evaluation
- Grant API access to integration partners
- Manage financial custom fields.

Does JobAdder Maintain any Security / Compliance Certifications?

Yes. JobAdder is certified to ISO 27001:2022. Certification is issued by Lloyd's Register Quality Assurance (LRQA) You can view our certification here.

©2024 Copyright JobAdder Operations Pty Ltd. All rights reserved.

Company summary

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.

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).

How often does JobAdder perform penetration tests and who performs them?

As part of our ISO 27001 certification, annual penetration testing is performed by CREST-certified tester on JobAdder's platform

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.

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 secure are JobAdder's data centres?

JobAdder's data centers are provided by AWS, which maintains ISO 27001 and ISO 9001 certifications:

- https://aws.amazon.com/compliance/iso-27001-faqs
- https://aws.amazon.com/compliance/iso-9001-faqs

A current list of its compliance programs and standards can be found here:

- https://aws.amazon.com/compliance/programs

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

- https://aws.amazon.com/trust-center/data-center/our-controls/

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"):

- https://aws.amazon.com/s3/sla/
- https://aws.amazon.com/messaging/sla/

©2024 Copyright JobAdder Operations Pty Ltd. All rights reserved.

Security FAQs

AI controls

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.

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/

Technology controls

How does JobAdder protect data-in-transit?

HTTPS using TLS 1.3 or above with approved secure ciphers is required for all web applications. Certificates are 2048-bit RSA.

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.

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.

©2024 Copyright JobAdder Operations Pty Ltd. All rights reserved.

Security 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 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.

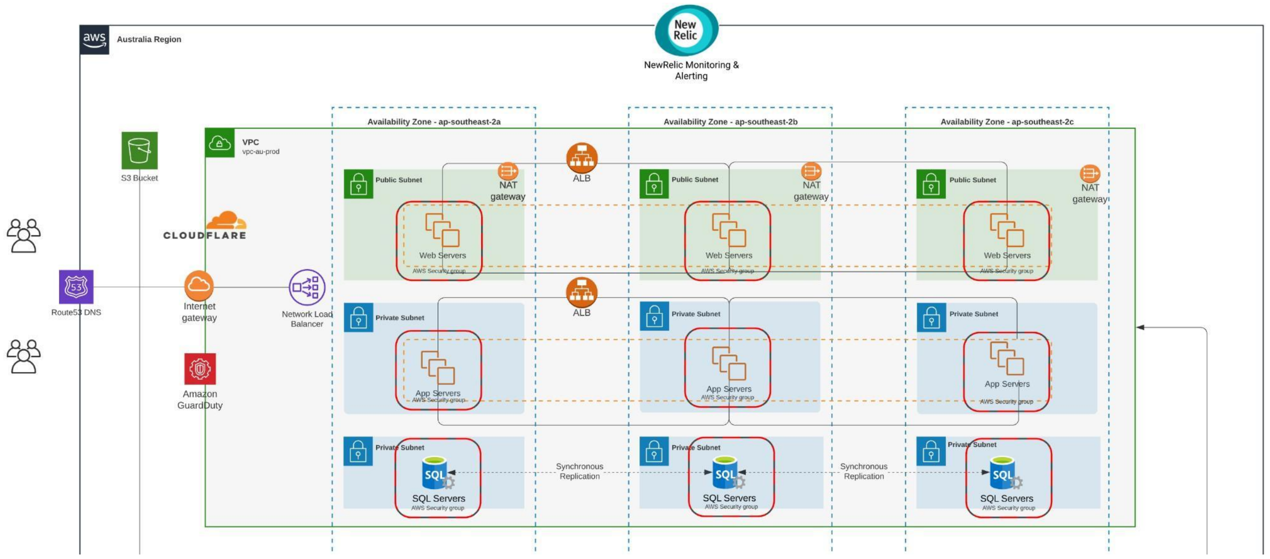
What logging, monitoring and threat detection controls are in place?

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.

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

How is JobAdder’s Application architected for resilience and availability?



©2024 Copyright JobAdder Operations Pty Ltd. All rights reserved.

Security FAQs

JobAdder's architecture is designed with multiple layers of resilience across our AWS infrastructure.

High availability is achieved through a combination of AWS-native redundancy and JobAdder's own infrastructure:

1. CloudFlare WAF for perimeter protection and DDOS mitigation.
2. 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 (ASGs) automatically replaces unhealthy instances and consistent application capacity.
4. Encrypted Amazon S3 is used for Document storage (resumes, cover letters, etc) which have a 99.999999999% (11 9's) of durability
5. Application Servers and databases run on encrypted EC2 and Amazon RDS. Data is mirrored asynchronously to a redundant server. Backups are managed and securely stored in AWS.
6. Backups are managed and stored securely in AWS. SQL Databases are backed up according to the following schedule:
   - Weekly full backup
   - Nightly differential backup
   - 15-minute transaction log backups
7. Recovery objectives
   - RTO is 2 hours
   - RPO is 15 minutes
8. Monitoring and metrics:
   - Cloudwatch for infrastructure and application metrics
   - New Relic for application performance and server-level monitoring.

Process controls

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.

©2024 Copyright JobAdder Operations Pty Ltd. All rights reserved.

Security FAQs

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 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.

How do JobAdder Administrators Authenticate?

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

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.

©2024 Copyright JobAdder Operations Pty Ltd. All rights reserved.

Security FAQs

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.

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

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

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.

What is your Disaster Recovery (DR) and Tests and Business Continuity Plan (BCP)?

JobAdder maintains ISO 27001-certified Disaster Recovery (DR) and Business Continuity Plans (BCP).

- Resilience is achieved through multiple regions and Availability Zones (AZ) so that if one AZ were to go down, there are two others that would continue in each region.
- Frequent back-ups to AWS Data Centres mean our BCP is tested continuously and the business would continue, relatively unaffected in a Business Continuity event.
- Disaster Scenarios are mapped and reviewed on an annual basis.
- Disaster Recovery testing is completed on an annual basis.

©2024 Copyright JobAdder Operations Pty Ltd. All rights reserved.

JobAdder

Adding Joy to the Job of Recruitment