Provida Security Statement

Last updated: 02/02/26

This document is intended as an attestation of Provida's security posture, in terms of our software as a service (SaaS) product. It is intended for our customers' decision makers and IT security personnel.

Provida is keenly aware that our business depends entirely on keeping our customer's data safe and secure, and we do this by incorporating strong security practices at every stage of the process.

1. Provida SaaS Production Environment

Provida uses an enterprise-grade secure, scalable cloud hosting environment to deliver high availability of its services, and to secure and protect client data.

All maintenance and configuration activities are conducted remotely by Provida employees.

Provida's cloud infrastructure is based upon Provida's custom multi-tenant application architecture. Separate databases per SaaS tenant ensure the necessary strong separation between data from different clients. All infrastructure responsibilities rest with Provida, and clients are provided with functionality to manage their own users and roles at the application level.

Provida employs industry standard practices and relies on its experience in operating highly secure SaaS solutions for security controls such as firewalls, intrusion detection, change management, and configuration management.

Scalability

Provida's cloud architecture, and the underlying AWS infrastructure, allows Provida applications to scale horizontally as the number of clients and volume of traffic increase. Provida uses multiple monitoring processes and tools to continuously track network resources, operating systems, applications, and capacity. Application servers are load balanced and can be scaled horizontally when required. Provida SaaS applications are hosted on a minimum of two application servers, for high availability and zero downtime deployments.

Databases

Provida uses Amazon's RDS (Relational Database Service) to host a highly scalable Postresql cluster consisting of multiple databases (database per tenant model). Automated processes ensure database patches are applied in a timely manner. Backups are automated and include both full backups and transaction logs going back 35 days. All data is encrypted at rest and in transit.

2. Risk Management

Provida business continuity planning includes practices to assist management in identifying and managing risks that could affect our ability to provide reliable services to its clients (as further described below). These practices are used to identify significant risks for the organisation, initiate the identification and/or implementation of appropriate risk mitigation measures, and assist management in monitoring risk and remediation activities.

Provida evaluates and manages risks related to its SaaS Solutions throughout their lifecycle, taking into consideration the consequences for our clients of loss of confidentiality or availability of the information we collect, process and store.

3. Security Policies & Organisation of Information Security

Policies

Provida maintains a SaaS Privacy Policy, updated annually, that explicitly addresses how Provida stores and protects client data and user data. Provida's business model is Software as a Service (we are not data brokers) and therefore all client data remains the property of the client and does not leave Provida's AWS cloud environment.

Information Security Coordination

Provida CTO (Chief Technology Officer) coordinates all security and privacy activities within Provida. Responsibilities of this position include:

- Driving security initiatives
- Policy review
- Security planning and program management
- Review effectiveness of the security program
- Coordinate Provida security incident response
- Perform periodic security audits and reviews

Provida CTO is responsible for policies and security implementation within the SaaS environment.

Segregation of Duties

Only authorised personnel can administer systems or perform security management and operational functions. Authorisation for and implementation of changes are segregated responsibilities wherever appropriate to the organisation.

4. Human Resources Security

Personnel Screening

Provida requires background checks on all personnel (including employees and contractors) at the time of hire or engagement. Provida also requires that all personnel sign non-disclosure and/or confidentiality agreements. Provida policy prohibits personnel from using confidential information (including client data) for any purpose outside their role, and this obligation continues after their employment or engagement ends.

A personnel member's failure to cooperate fully in any background check and any dishonesty or omission of information pertaining to a background check precludes employment or engagement with Provida.

Terms of Work

Provida operates an onboarding process for all personnel, including at a minimum the following steps:

- Communication of policies, code of conduct, and behavioral standards to personnel
- Signature of the appropriate agreement (employment agreement or contract agreement) that includes a confidentiality agreement and acknowledgement of Provida's Information Security Policy
- Background checks
- Security and privacy awareness training

Termination of Work

Provida maintains a formal termination process that, promptly upon termination or change of work, requires return of all Provida and client assets, disables or adjusts access rights, and reminds personnel of their remaining contractual obligations. All access (logical and physical) is terminated on or before the termination date.

5. Asset management

All data collected by Provida on behalf of its clients is the property of the respective clients and classified as highly confidential. Provida provides employees with the necessary guidance for the handling of all information according to its classification. Client data is logically separated from other clients. Access to client data is restricted to legitimate business use only.

Client Data Location

All client data is processed and stored in AWS Sydney data centre. Any change to this would require notification to all clients.

Media Handling

Provida Information Security Policy prohibits copying client data on removable media device, including flash drives, hard drives, tapes, or other media, other than for legitimate business purposes.

The client can request their data at any time.

Provida deletes all client data following termination of the SaaS contract.

6. Access Control & Physical Security

Provida CTO manages access control policies and procedures for the corporate network and access control policies and procedures for the SaaS production network.

User Access Management

Accounts on Provida SaaS production network, including for network administrators and database administrators, are mapped directly to employees using unique identifiers based on staff names. Generic administrative accounts are not used. As part of the formal termination notification process, all physical and system accesses are immediately adjusted to the new role or revoked.

Password complexity rules and account lockouts are enforced in all environments to protect against brute force dictionary attacks or other passwords threats.

Provida periodically reviews staff access to internal systems. Reviews ensure that staff access rights and access patterns are commensurate with their current positions.

User responsibilities

Provida Information Security Policy requires staff to notify their manager immediately if they believe that the security of their password has been compromised. Employees must abide by all Provida policies, including all sections of the Information Security Policy.

System and Application Access Control

Authentication and robust access controls ensure that all clients' confidential information is secured against unauthorised access. Users of Provida SaaS Solutions must be authenticated before they can access their data, and rights associated to their credentials control access to the logical structures containing their data.

Accesses to resources are controlled by explicit rights in all environments. Personnel are given appropriate accounts on systems which they are authorised to access following the "least privilege" principle. Cloud infrastructure access controls are provided by AWS IAM.

Two-factor authentication is required for remote access and for access to production environments. Further, separate accounts are used to access production environments which are only provided to authorised personnel.

Access to client data is limited to legitimate business need, including activities required to support clients' use of the SaaS Solutions. Personnel may only access resources relevant to their work duties.

Data Access by Clients

Client end users are authorised to access and edit only the data relevant to them.

Client end users are identified with an email address. All passwords are securely hashed. They authenticate to the system over an HTTPS connection with a time-limited secure code via email.

Access control to program source code

Write access to Provida SaaS production source code is limited to the engineering staff. Anti-malware scans are performed during build processes.

7. Physical and Environmental Security

Provida SaaS Solutions utilize Amazon Web Services (AWS) for production and test/staging. AWS operates extremely secure data centres with strict physical security measures, including 24×7 security guards, electronic key systems, biometric access, and CCTV.

8. SaaS Operations Security

Provida SaaS Solutions infrastructure employs industry best practices such as default deny rules for firewalls, intrusion detection systems and automated patch management.

Operational Procedures

Provida maintains operational procedures that include at a minimum:

- security control measures for all systems in the environment

- hardening – disabling of all non-essential processes and ports, removing all default users
- patches deployed promptly on all applicable systems per manufacturer recommendation, and no more than within 3 days for critical security patches for internet facing applications

Separation of development, testing and operational facilities

All access is limited to the least privilege needed and requires authentication. Access logs are reviewed at least quarterly.

Administrative access to SaaS Operations resources is limited to SaaS Operations personnel and authentication requires a separate set of credentials.

Protection against Malware

Provida deploys anti-malware software with automatic scanning and update on all workstations and scans all code for malware.

Updates are managed and pushed out via workstation/server policy management. Definitions are automatically updated.

Provida uses a leading commercial solution for email security (Microsoft 365), including incoming and outgoing filtering for spam, phishing attacks and malware.

Data Backup

Provida stores all client data in the SaaS production environment on highly available and redundant storage systems. Database backups are stored on AWS S3 for 35 days, then automatically deleted. Provida can restore client data (on request) to any day in the last 35 days.

Logging and Monitoring

Provida maintains audit information and logs application interactions, monitors these logs for abnormal pattern and unauthorised access attempts. Logs are centralised in a limited-access system that prevents deletion and changes. Logs are retained for 90 days before automatic deletion.

Provida will ensure the timely communication of significant security/privacy incidents through the management chain and ultimately to any affected client.

Technical Vulnerability Management

Manual and automated vulnerability testing are performed during the development process. Provida performs regular automated application penetration testing of its Solutions.

Vulnerabilities are logged as defects, resolved, or mitigated, and verified fixed.

Patch Management

Reviews performed on a regular basis ensure patching is consistent and current based on industry standards. Provida deploys security patches released by the vendors as necessary to development, testing, and production systems after validation in pre-production environment.

Critical patches are evaluated and deployed as promptly as possible. Patch applicability and urgency is evaluated based on the zone of deployment (perimeter, DMZ, applications, storage), its relevance (i.e., is the service being patched enabled in the environment) and threat severity (likelihood x impact).

Encryption of Data

All data is encrypted in transfer and rest with industry standard protocols and cyphers. HTTPS is enforced on all sites and data collection endpoints. Database backup storage systems utilise disk encryption. SSL/TLS certificates for public web sites are rotated automatically on an annual basis.

9. Communications Security

SaaS Network Security Management

Application logging and monitoring facilitates alerting, analysis, and risk assessment.

Segregation in Networks

Provida production infrastructure uses separate segments for the web and storage layers with a firewall configuration between the Internet and the demilitarized zone (DMZ).

Information Transfer

Provida clients access the Provida environment via the public Internet. All data transfers from Provida SaaS Solutions must use secure protocols; all data transfers to Provida SaaS solutions require secure protocols.

Confidentiality and Non-Disclosure Agreements

All Provida personnel must sign the Provida Confidentiality Agreement at the time they join the organisation. Upon termination, personnel are provided another copy of their agreement.

Provida requires a non-disclosure agreement or confidentiality clauses in all contracts of third parties accessing computing facilities or information assets as well as prior to sharing or providing access to any confidential information outside of Provida, whether verbally or in writing.

10. System Acquisition, Development and Maintenance

Security in Development and Support Process

Provida follows an agile development methodology in which products are deployed on an iterative, rapid release cycle. Security and security testing are implemented throughout the entire software development lifecycle.

Provida uses defense-in-depth best practices and validates them using both internal and third-party security vulnerability scans.

The internal quality assurance function also regularly reviews application endpoints for vulnerabilities, including those identified in OWASP Top Ten.

The development process includes a review of all embedded third-party components to ensure that security updates are incorporated. Use of open-source software is subject to technical review and approval.

11. Supplier Relationships

Provida may use contractors for development and testing tasks. These individuals work under the direct supervision of Provida employees.

12. Incident Process

Provida technical support will notify client contacts assigned to the account as soon as possible after confirming them as being affected by a security or privacy breach or by a DR event, but in any event within 24 hours for significant events and within 2 business days for non-critical events.

13. Business Continuity & Disaster Recovery

Redundancy

Provida maintains client data within the SaaS production environment on fully redundant, replicated storage systems (AWS EBS and S3). Provida SaaS Solutions extends redundancy beyond storage through the entire infrastructure, from load balancers and processing engines to power and telecommunication providers. Specifically:

- Each application server is independent and scaled to three times its daily average traffic. Unavailability of any single application server does not result in any noticable failure as the other application server instances automatically adjust and are scaled to absorb the load from the failed instance(s).
- A failure in the primary cloud region may involve some manual intervention on the part of the Provida SaaS Operations team depending on the level of severity and complexity of the issue. In the unlikely event of complete cloud data centre failure, the SaaS Operations team has instructions and recovery steps to bring the solution back online in the most expeditious manner at an alternate region if necessary. Clients will be notified of any change in data centre region.

14. Compliance

Provida complies with statutory and regulatory requirements and uses reasonable efforts to comply with applicable industry standards.

15. Privacy

Please see the Provida SaaS Privacy Policy.

Authority

Dave Bartlett

Chief Technology Officer

Provida Ltd.