Zambion – Security Policies and Processes

READYTECH
READY TO PUT PEOPLE FIRST

Table of Contents

Introduction

Zambion is a state of the art, web based Payroll, HR, Time and Attendance, Leave Management Software that is ATO compliant, intuitive, intelligent, and easy to use. Making sure your data is secure and protecting it is one of ReadyTech's most important responsibilities. We're committed to being transparent about our security practices and helping you understand our approach.

Security and Compliance

ReadyTech has established an industry-leading security program, dedicated to ensuring customers have the highest confidence in our custodianship of their data. Our Information Security Management System (ISMS) is aligned to the ISO 27000 standards and is regularly audited and assessed by third parties.

Our ISO 27001:2013 certificate is available on the JAS-ANZ register:

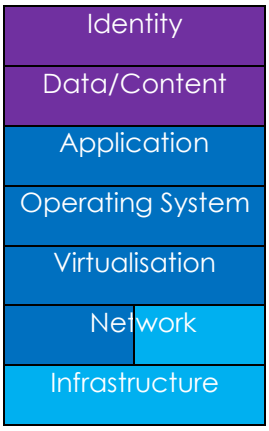
https://www.jas-anz.org/our-directory/certified-organisations/0094c63d-cd23-487a-9991-4d782779de46

Shared Security Responsibility Model

ReadyTech strives to protect the confidentiality, integrity and availability of all critical information and stored customer data.

While we manage security *of* the application, security *in* the application is the responsibility of the customer. Zambion is provided as software-as-a-service, i.e., a fully functioning modern web application. ReadyTech is responsible for procuring, configuring, monitoring and maintaining all aspects of the computing environment, from the servers to the application.

The customer is responsible for managing the access of their authorised users, password policies and configuring roles and permissions within the application itself.



Physical

	Customer Responsibility	Security **in** the application
	ReadyTech Responsibility	Security **of** the application
	Infrastructure Provider Responsibility	Security **of** the cloud

Infrastructure

Zambion is hosted in a private cloud with Equinix. Equinix provides state-of-the-art data centers and a world-leading compliance program. Equinix operates, manages and controls the components from the internet gateway layer down to the physical security of the facilities in which Zambion operates.

Data Sovereignty

Zambion only uses the Equinix Sydney and Melbourne based data centers to ensure data is stored and processed within Australia. Data and services are replicated across both locations for high availability.

Data Ownership

The customer always owns their data. ReadyTech collects and processes data on behalf of the customer as required to provide and support the platform, as further detailed in the Privacy Policy: https://www.readytech.com.au/privacy

Personnel Security

All ReadyTech staff undergo screening checks before employment including reference, qualification and police checks. Security awareness training is provided at initiation and continuously throughout the year. Staff with privileged access to systems or data receive additional job-specific training on privacy and security. Personnel requiring access to production systems or client data are required to have undergone appropriate security clearances.

ReadyTech has appointed a Chief Information Security Officer who is responsible for the performance of the ISMS. All staff have security responsibilities assigned as part of their roles.

Identity and Access Management

Zambion provides out of the box functionality to support secure access control for customers:

- MFA (Multi-Factor Authentication) for password-authenticated users
- Active Directory Services for use with Single Sign On
- Role-Based Access Control (RBAC) for configurable, granular provision of permissions and functionality to users.

When the system is configured to use the native password authentication, password length and complexity requirements are enforced by the system. Password expiration can be configured or disabled entirely.

Access for ReadyTech staff to the application and infrastructure is provided on a least necessary privilege basis, with technical controls limiting access to approved staff, on compliant corporate devices validated with MFA. All staff devices including laptops and mobile devices are centrally managed in the device management system to ensure they meet ReadyTech standards which includes device encryption, password policies, malware control and time limited screen locking.

Standard Operating Environments

ReadyTech uses a documented Standard Operating Environment for all servers. Any change to the environment goes through a structured change management process.

Patch Management

Server operating systems updates are applied on a monthly basis, with critical security updates applied when necessary. Application vulnerabilities are identified through automated systems. The patching and upgrade of software components is incorporated into regular software development procedures and release schedules.

Critical issues and security patches may necessitate an out-of-cycle release, but these are processed through standard change management workflows.

Software Development

ReadyTech uses a Secure By Design approach in our Software Development Life Cycle. Security is considered in the design, development and testing of our software. We use a series of software development environments including development, staging and production. Software is only able to progress to the next environment after it passes all the checks at each level including mandatory internal peer code review, static code analysis, automated unit and integration testing, manual QA and UAT.

Access to release branches in the code version repository is strictly limited. ReadyTech use static code analysis tools to identify known vulnerabilities in developed code, conducted as part of the automated build pipeline.

ReadyTech web applications are developed using security best practice. All developers are trained to be aware of OWASP security guidelines. Database queries are parameterized. Application inputs and outputs

are properly sanitised and encoded. Errors and exceptions are logged and monitored. User authentication passwords held within the database are stored salted and hashed.

Database Systems

Each customer uses a logically isolated database. Databases are securely provisioned with unique credentials per customer ensuring secure data partitioning. All use and administration of the database is through the web application frameworks minimizing any exposure through direct database access.

The network is designed to restrict access to the database to the fewest necessary systems. All database data is encrypted at rest using AES-256 with secure key management procedures.

Production, test and development environments are strictly separated on both the database and application server basis.

Network Security

Network access to the production environment from open, public networks (the internet) is restricted. Only required network protocols and ports are exposed to minimize the potential attack surface for malicious actors. Changes to the production network configuration are restricted to authorised personnel and all changes logged.

Multitenancy: the network and application layers are shared but each customer uses a logically isolated database and object storage in an isolated namespace.

Cryptography

Data at rest, and in transit, is only encrypted with ASD Approved Cryptographic Algorithms (AACAs) and ASD Approved Cryptographic Protocols (AACPs).

Transport Layer Security (TLS) is used for all public network connections with a modern security policy meeting an SSL Labs A rating. The preferred server negotiated connection will be on TLS 1.2 with Elliptic Curve Diffie-Helman session keys and perfect forward secrecy. SSLv3, TLSv1.0 and TLSv1.1 are disabled. HTTP Strict Transport Security (HSTS) ensures that a TLS connection is always used.

Structured data stored in our Databases is encrypted at rest using AES-256.

Logging and Monitoring

Site uptime, host and application performance is monitored by independent third-party services with operational alerting and response procedures in place. Regular governance meetings and performance review ensure the ongoing performance and availability targets are met.

Penetration Testing

ReadyTech engages independent, CREST certified entities to conduct application penetration tests annually. Results of these tests are shared with ReadyTech management and available to customers under NDA. Findings are reviewed, prioritised and tracked to resolution. Customers wishing to conduct their own penetration test of the Zambion application should obtain permission from ReadyTech.

Backup Management

The database operates on the SQL Server service. Transaction log backups offer a Recovery Point Objective (RPO) of 5 minutes. Multi Availability Location replicas provide a hot synchronous standby with a Recovery Time Objective (RTO) of approximately 30 minutes in the case of catastrophic failure of the master database. Complete logical backups of the database are stored daily.

Data Retention

Data is retained within the system for the life of the contract. At contract termination, data is returned to the customer and permanently destroyed according to standard operating procedures. Data will be made available in standard, documented formats via the platform.

Database backups are retained for 30 days and deleted by automated lifecycle policies.

Business Continuity

The concepts of business continuity and disaster recovery are integrated into our design and architecture of highly available systems in the public cloud. Failure is routinely expected, planned for, tested and managed with automated systems and redundancy.

Resilience and scalability are addressed on AWS through:

• Running multiple database server instances in multiple Availability Zones (distinct locations that are engineered to be insulated from each other)

• Application layer availability and scalability managed through Kubernetes across both locations

Data and assets are versioned, backed up and monitored.

Incident Management

ReadyTech has documented Incident Response, Business Continuity, Disaster Recovery, Security and Data Breach Response, and Crisis Management Plans that are tested at least annually.

Clients will be notified in accordance with our Incident response or Data Breach response plans in the case of an incident, the timing of which is outlined in the relevant plans and is based on the severity and urgency. The nominated role at ReadyTech will continue to communicate with the customer on the specified schedule at a minimum until the issue is resolved. In general, ReadyTech takes the approach of informing the customer as soon as is practical in all cases.

Third Party Supplier Management

ReadyTech relies on sub-service organisations, such as Equinix, to run its business efficiently. We evaluate and qualify our vendors with a risk-based approach and documented standards which include security, technical and financial assessments. ReadyTech ensures our security posture is maintained through legal agreements and regular security compliance review of these arrangements.

Contacts

ReadyTech is continually striving to keep our systems secure. If you become aware of any security issue or have any further queries regarding this document, please contact the security team directly at security@readytech.io.

Classification

This document is **Public**; it is approved for public release.

Version Control/Revision History

Version	Date	Initials	Description
1.0	31/05/2021	AK	Prepared for distribution