MyHR® CONFIDENTIAL

MyHR Security & Privacy Summary

Updated Dec 2025

At MyHR, the trust that our customers place in us to safeguard their people data is fundamental to how we design, build, and operate our platform. This document provides an up-to-date overview of our security and privacy controls across infrastructure, identity, data protection, monitoring, incident response, and governance.

---

1. Infrastructure & Hosting

Cloud Hosting

- MyHR is hosted on **Amazon Web Services (AWS)** in the **ap-southeast-2 (Sydney)** region.
- The solution is architected as a **multi-tenant SaaS platform** with strict logical boundaries using customer authentication and customer-scoped storage.

Core Components

- **Compute**: ECS Fargate (microservice architecture) and supporting Lambda functions.
- **Databases**: RDS MySQL (Multi-AZ), ElastiCache Redis for session/caching layers.
- **Storage**:
    - **Primary file storage is S3**, with enforced encryption, TLS, and versioning.
    - Ongoing migration of legacy EFS data to S3 to support improved security (malware scanning), resiliency, and restore capability.
- **Networking**: Dedicated VPCs per environment, security groups for service segregation, ALB for traffic termination at origin.

Edge Security

- **Cloudflare** provides DNS, CDN, WAF, bot protection, DDoS protection, and Zero Trust access to internal-only tools.

High Availability / Redundancy

- Multi-AZ redundancy across compute, RDS, Redis, and S3.
- Customer data is stored primarily in AWS Sydney. Any processing or storage outside this region occurs only via approved third-party sub-processors operating under contractual and security controls.

---

2. Identity, Authentication & Access Control

Internal Access

- Access to AWS, internal tools, and DevOps systems is controlled via **Google Workspace SSO** with **MFA required**.
- AWS human access uses **SSO + role assumption** (Control Tower managed).
- **Local development** access also uses the same SSO/role-based model (IAM users removed).

Client Access

- Clients authenticate via secure username/password.
- **Password controls**:
  - Minimum 12 characters
  - Supports at least 64 characters
  - Strength-based evaluation (no enforced composition rules)
  - Prevents common/guessable passwords and “MyHR” variants
  - Stored via salted, one-way hashing

Access Governance

- Least-privilege principle applied for all environments.
- DevOps access restricted to senior engineers.
- Control Tower and CloudTrail provide full access auditing.

---

3. Secrets Management

- **1Password** is the primary store for secrets with **ESC integration** for IaC (Pulumi).
- Separate vaults per environment with distinct access rules.
- Secret rotation tracked in a **Notion rotation database** including procedures, frequency, and last rotation.
- Rotation is manual issuance with automated application through IaC.
- Secret access recovery via Ops + IT360; DevOps automation vault handled separately.

---

4. Data Protection & Privacy

Data Residency

- All customer data is stored exclusively in **AWS Sydney (ap-southeast-2)**.

Encryption

- **In transit:** TLS 1.2+
- **At rest:** AWS-managed AES-256 encryption across RDS, S3, EFS, and other supported services.

PII Scope

- MyHR stores typical HR information, including contact details, employment records, tax IDs, and bank account numbers.
- **No biometric or medical data** is collected or stored.

Privacy Practices

- MyHR complies with NZ, AU, and CA privacy laws.
- Platform designed to avoid logging sensitive fields (e.g., passwords).
- Retention aligned with legal HR record-keeping requirements (e.g., 7 years).
- Customer off-boarding triggers structured data deletion.

---

5. Backups, DR & Business Continuity

Backups

- **RDS point-in-time recovery (PITR)** with an effective **RPO of 5 minutes**.
- **S3 versioning** enabled to restore deleted or overwritten objects.
- Automated and periodic restore testing performed.

Disaster Recovery

- **DR plan reviewed annually**.
- **Bi-annual tabletop exercises**, plus scenario-based restore tests with Lancom.

Recovery Objectives

- **MAD:** 24 hours
- **RTO:** 4 hours
- **RPO:** 5 minutes

6. Monitoring, Logging & Threat Detection

Monitoring

- Centralised observability on **Datadog us1** including:
  - Infrastructure metrics (CPU/memory/latency)
  - RDS replication lag, lock contention
  - Redis utilisation
  - APM for service-level bottlenecks
  - Synthetic monitoring for key user flows
  - EFS (where still in use) and S3 security events
  - Certificate expiry

Threat Detection

- **Cloudflare WAF** and DDoS protection.
- **AWS GuardDuty** for continuous threat detection.
- **Detectify** for automated OWASP-aligned vulnerability scanning.
- Logging through CloudTrail and Datadog for audit visibility.

Alerts & Incident Handling

- Critical alerts → **PagerDuty** (24/7 engineering on-call with Lancom backup).
- Medium/low alerts → Slack.
- Incidents are **manually declared** in Datadog and fully documented with RCAs.

7. Vulnerability Management & Secure SDLC

- **Annual penetration testing** by CyberCX.
- Findings reviewed, prioritised, and remediated based on severity.
- CI/CD pipeline (GitHub Actions) enforces:
  - Automated tests
  - Static analysis
  - Linting/formatting
  - Type checks
- Detectify handles continuous vulnerability scanning.
- Code changes require peer review with specific code owner checks.

8. AI Governance & Responsible Use

AI Platforms

- Primary GenAI execution runs on **AWS Bedrock**, isolated to MyHR's environment and not used for model training.
- We also have available **Azure OpenAI** in a private configuration (no customer data used for training) for evaluation purposes.

Safeguards

- Human-in-the-loop validation for workflows affecting HR outcomes.
- In-product transparency notices.

---

9. Physical & Device Security

- Offices in Auckland (leased), Christchurch/Sydney/Squamish (shared spaces).
- Visitor sign-in/out and badge controls.
- Company laptops managed via **MDM**, including patching, device encryption, and automated cleanup of downloads.
- Endpoint protections: **Huntress**, Cloudflare WARP when offsite.
- Bi-annual staff security/privacy training.

---

10. Third Parties & Sub-processors

Key sub-processors include:

- **AWS** (hosting, storage, compute)
- **Cloudflare** (CDN, WAF, DNS, security)
- **Datadog** (monitoring, logs, SIEM)
- **1Password** (secrets management)
- **Lancom** (DevOps partner, monitoring/IDP changes)
- **CyberCX** (security testing, advisory)

A full sub-processor list is available on request.

---

11. Support & Incident Response

- Customer support during business hours.
- Engineering on-call **24/7**.
- Incident RCAs documented in Datadog notebooks.
- Monthly reviews of incidents and monitors.
- Internal status page tracks service health.

---

12. Current & Upcoming Improvements

- Continuing migration from EFS → **S3 + malware scanning**.
- Ongoing SOC 2 readiness using Sydekick by **Onwardly**.
- Improved secret rotation automation.
- Planned expansion of client authentication options (future SSO support).
- Expanded DR tabletop exercises and AI audit improvements.

Contact

Security & Privacy: pete@myhr.works

General DevOps Queries: devops@myhr.works

Support escalates internally where required.
