enableHR®

Privacy & Security Technical Overview

FCB GROUP

FCB WORKPLACE LAW

FCB HR

FCB SMART VISA

HR ASSURED
smarter workplace solutions

ENABLEHR- PRIVACY & SECURITY TECHNICAL OVERVIEW

Contents

1 Introduction

enableHR provide an easy-to-use online platform for businesses and their partners through a cloud based HRIS platform and software.

enableHR is part of the FCB Group. FCB Group assists many businesses with their employment and human resources needs including around hiring, managing and exiting of their staff and core legal compliance requirements.

This document provides a technical overview of the controls and policies in place to protect customer data within enableHR.

1.1 Who is enableHR?

When we refer to "we" (or "our" or "us'", that means:

- **enableHR Pty Ltd** – Australia (ABN: 84 123 231 005);
- **enableHR Limited** – New Zealand (NZBN: 9429041375488); and

Our Head Office is in Sydney, Australia, but we operate and have offices across Australia and New Zealand.

1.2 Primary Contacts

Name	Email	Description
Campbell Fisher	cjf@fcbgroup.com.au	Managing Partner, FCB Group
Jessica Fisher	jmf@fcbgroup.com.au	Head of Risk, FCB Group
Martin Lau	msl@fcbgroup.com.au	Chief Technology & Innovation Officer, FCB Group

2 Application & Infrastructure Security

The following sections describe the application and infrastructure level security controls and processes in place to protect client data.

2.1 Hosting Providers

Our primary application hosting is through Amazon Web Services with all data and services delivered from the Asia Pacific (Sydney) Region. Amazon Web Services are certified under the ASD Certified Cloud Services List (CCSL) for unclassified data.

Our disaster recovery hosting is through ASE IT, also an Australian based infrastructure provider, with physical servers managed through NextDC's data centre in Sydney.

2.2 Infrastructure Security

All access to our infrastructure is by VPN (OpenVPN) using 2 Factor Authentication (Yubikey). Once connected to the VPN, host level access is managed based on SSH Private / Public Key authentication. Access to specific hosts is restricted based on the need of staff based on their job function.

Nodes within our infrastructure run a baseline level of CentOS with security patches applied on a 3-month schedule. Unplanned or critical patches are applied as needed.

2.3 Network Segmentation

Our application networks are logically segmented to provide partitioned hosting of:

- Front-end load balancing and SSL termination
- Public website hosting
- Application delivery
- Data storage

Access between tiers is allowed based on whitelisted rules, enforced through both core network routing and firewalls as well as per-host firewall rules.

2.4 Infrastructure Redundancy

We maintain redundant systems within our primary hosting provider (Amazon Web Services) as well as with our disaster recovery provider (ASE IT). Within each provider, we maintain redundant storage of all data, as well as application hosting.

Capacity of both storage and application processing is continually monitored and adapted to ensure we are able to meet customer need based on business as usual requirements, as well as being able to handle failure situations, ensuring we have sufficient spare capacity to share load across nodes in the event that some nodes go offline.

2.5 Application Security

We undertake annual penetration and vulnerability testing through independent third-party security services. These tests include both automated and manual application and network testing of all applications managed by us.

We incorporate vulnerability scanning in our build processes to ensure up-stream components and libraries which we depend on are free of known vulnerabilities.

Our development processes (see "2.6 - Quality Testing" below) incorporate checks to address application security concerns through maintenance and feature development.

2.6 Quality Testing

We follow best-practice development processes where source code is authored and reviewed by our internal development team prior to being merged into the main working code base. These changes include a range of automated tests, which are executed prior to being promoted through to our test environments.

Changes made to test environments are then tested by our product team to ensure the continued operation of existing capabilities as well as proper function of new capabilities.

Packages are promoted through environments without alteration. Any environment specific variation is encapsulated through configuration, which is managed as described in "2.7 - Change Control & Configuration Management" below.

2.7 Change Control & Configuration Management

All source code is managed through Git with centralised hosting through an external provider. Infrastructure changes and application configuration are also tracked through Git and deployed via Ansible.

Our applications are built through automated build processes and packaged into Docker images for deployment.

Docker images are deployed to non-production and production environments through automated processes leveraging Ansible. The same package is built and promoted through our non-production to production environments.

While deployments are automated, they are initiated by an operator, who oversees the process and is able to remediate should an issue occur throughout that deployment.

2.8 Release Schedule

We classify releases into three categories:

- Hotfix releases which address minor issues;
- Maintenance releases which introduce small improvements or functional changes; and
- Feature releases which introduce large changes to our applications and processes.

Our standard process is to deploy these releases outside of core operational hours (07:00 in New Zealand to 17:00 in Western Australia). This means that releases are performed around 21:00 Sydney local time.

When a system outage is necessary (for example, a change requires a change to the database schema) we undertake these changes on a Friday evening, at the time outlined above. When such an outage is scheduled, notifications are provided within our applications for the hours leading up to the outage.

For feature releases which contain significant changes to application functionality to deliver improved usability, we communicate those upcoming changes to users via email communications in the weeks preceding the change, and in-application messages in the days preceding the change.

2.9 Application Level Configuration

Our HRIS system can be configured by clients who wish to tailor their own specific account to strategically align with their own defined HR and safety processes and template documentation. Configuration is undertaken by our Client Experience and Implementation team of consultants who manage and control the technical build from the back-end of the system. Authorised consultants are required to access and log into client accounts for valid purposes only, which include carrying out the technical work, undertaking troubleshooting, completing testing and activating approved configuration. All work undertaken by our consultants undergoes peer review processes and is authorised and approved for quality assurance purposes by the client. All configuration projects are managed according to our project management methodologies which track performance against the scope, budget and timeframes set for the project.

3 Information Management

The following sections describe the protections and controls in place to specifically manage customer data.

3.1 Data Encryption & Redundancy

3.1.1 In Transit Encryption

All ingress traffic to our systems is encrypted by TLS:

- End-user access by HTTPS; and
- System-to-System access via SSH/SFTP or HTTPS.

Where possible, all egress traffic is also encrypted via TLS:

- End-user access is always by HTTPS;
- System to System access is always by SSH/SFTP or HTTPS; and
- Email delivery is by SMTPS when available (using opportunistic security if the recipient SMTP server supports TLS) otherwise standard SMTP is used.

3.1.2 At Rest Encryption

Any filesystem containing customer data (whether that data be in the form of actual files, binary stores such as database data files, or logs containing user request / response information) are encrypted using LUKS (Linux Unified Key Setup) Disk Encryption.

3.1.3 Data Redundancy & Validity

All block devices (disks) are configured to provide redundancy across a given filesystem, with that filesystem also replicated across hosts.

For traditional file storage, this is done through BTRFS (redundant local disks and cross-host replication). BTRFS provides file checksums to ensure the consistency of data over time.

For database storage, this is done through LVM with separate storage for Write Ahead Logs (WAL) and host level replication of those data files (BTRFS is not used due to the poor performance characteristics of journaling filesystems with user-space managed binary repositories)

3.2 Data Retention

3.2.1 Backup Processes & Retention

All data is backed up hourly, with those backups being hosted on infrastructure within both our primary data centre and our disaster recovery provider. Hourly backups are merged into a daily backup overnight and retained for 6 months.

In a worst-case scenario of a catastrophic failure in our primary data centre, immediately before a backup was about to commence, the maximum data loss would be 1 hour.

3.2.2 Soft / Hard Deletes

Where possible, our applications implement soft deletes (marking pieces of information as deleted and supressing from display rather than physical removal of that information) to remove end-users' data. As a result of this mechanism, most data is retained indefinitely through our systems, with that retention also mirrored through our backup processes.

On request by customers, data can be hard deleted (that is physically removed from our physical storage). When data is hard deleted, it will still exist within our backups – but will naturally expire as those backups continue to roll-over.

3.3 Information Classification

Our systems provide management of a range of Personally Identifiable Information (PII) and Sensitive Information (SI).

Access to these systems is by:

- Customers where access is controlled by our in-application role-based access control (RBAC) where permissions are applied to roles and roles to users;
- Our application administrators who have access to customer accounts and are able to impersonate users within accounts to provide support. Administrator access can be restricted on request to specific named administrators.; and
- Technical staff who are able to access the underlying infrastructure and services, bypassing the application based RBAC above. Access at this level is restricted to staff needing to provide technical operational support to those systems, where access is controlled as discussed above in "2.2 - Infrastructure Security".

Production data is replicated to lower environments as needed based on development and support needs. These environments are managed in the same way as the production environment, with the same access controls in place.

3.4 Auditing & Logging

Our applications capture and store request and response logs which provide full details of individual users undertaking actions through our systems. Additionally, in-application auditing provides a second level of audit process for key changes within the application.

4 Business Continuity

The following sections outline the procedures we have in place to ensure business continuity in the face of catastrophic failure scenarios.

4.1 Application, Infrastructure & Support BCP

We have documented BCP plans for handling the catastrophic failure of our primary (Amazon Web Services) infrastructure and the process to fail over to our disaster recovery site (ASE IT). The consistency of backups and the ability to restore those backups is regularly tested.

4.2 Risk & Breach Management

We maintain a documented procedure to manage the risk and remediation in the situation of an information security breach.

5 Further Information

For further information relating to our privacy and security, please contact the relevant support channel:

- privacy@enablehr.com for enableHR requests

6 Revision History & Update Policy

The contents of this document should be reviewed at a minimum on an annual basis, but also as other fundamental changes to enableHR's service, infrastructure or applications dictate. The changes resulting from those reviews should be documented in the table below.

Version	Date	Author(s)	Comments
1.0	9 November 2018	Martin Lau	Expanded on previous "Security & Compliance" information document to provide more specific information across a range of areas.

enableHR®

enablehr.com

BRISBANE
Level 5, 300 Ann Street
Brisbane QLD 4000
Phone 07 3046 2100

SYDNEY
Level 11, 83 Mount Street
North Sydney NSW 2060
Phone 02 9922 5188

MELBOURNE
Level 18, 607 Bourke Street
Melbourne Vic 3000
Phone 03 9098 9400

FCB GROUP | FCB WORKPLACE LAW | FCB HR | FCB SMART VISA | HR ASSURED™ smarter workplace solutions