QuickHR Trust Brief 2026

Enterprise Security, Compliance & Cloud Assurance
By Enable Business Pte. Ltd. – Singapore

01 Executive Summary

QuickHR provides a fully hardened, cloud-native Human Resource Management System designed for organisations that require uncompromising security, privacy, and operational resilience. Our platform is independently audited, certified against internationally recognised standards, and architected using enterprise-grade controls across every layer of the stack — from infrastructure and application security to data governance and disaster recovery.

This Trust Brief outlines QuickHR's security posture, cloud architecture, compliance framework, and the controls that safeguard employee data throughout its lifecycle.

02 Certifications & Independent Verifications

QuickHR's security program is externally validated and audited annually.

ISO 27001:2022 — Certified

Comprehensive Information Security Management System (ISMS) covering infrastructure, application, and operational processes.

MTCS SS 584:2020 Level 2 — Certified

Singapore's Multi-Tier Cloud Security standard verifying strong cloud service controls, configuration hardening, and tenant-level isolation.

SS 714:2025 (DPTM) — Certified

Singapore Data Protection Trustmark certification validating end-to-end data lifecycle governance, privacy controls, and PDPA-aligned processes.

PDPA Compliance — Certified

Full compliance with Singapore Personal Data Protection Act, including consent management, data minimisation, access control, incident reporting, and secure disposal.

All certifications are audited by accredited external assessors annually.

03 Cloud Infrastructure & Security Architecture

QuickHR is hosted on Amazon Web Services (AWS) – Singapore Region (ap-southeast-1) and follows a multi-layered defense-in-depth model.

Perimeter Security

- Web Application Firewall (WAF) with custom rule sets
- DDoS protection at both network and application layers
- TLS 1.2+ encrypted traffic with load balancing

Network Architecture

- Private subnets with no public internet access to databases
- Network segmentation and microsegmentation
- Dedicated VPCs aligned with internal baselines (QHR-UHS 3.0 & AHS 1.0)
- Security groups enforcing least-privilege traffic flows

Application Layer Security

- Multi-factor authentication (MFA) for administrative access
- Role-Based Access Control (RBAC) with least-privilege permissions
- Argon2id password hashing hardened with peppering
- Continuous vulnerability scanning and patching (VA testing)
- CREST-certified penetration testing (annually)

Data Protection

- AES-256 encryption at rest
- TLS 1.2+ encryption in transit
- Database encryption with AWS KMS key management
- Automated encryption key rotation

Logging, Monitoring & Detection

- SIEM monitoring with real-time alerting
- Immutable logs encrypted using AES-256 to prevent unauthorized access and tampering.
- Structured access logging for all privileged activities
- Continuous vulnerability scanning

04 Data Lifecycle Management

QuickHR adheres to internationally accepted data lifecycle best practices.

Data Collection

- Data minimisation and purpose limitation
- Consent captured and managed according to PDPA requirements

Data Processing

- Segregated environments (production, staging, development)
- Strong authentication and access attribution for all privileged access
- Privacy by Design embedded throughout SDLC

Data Storage

- Encrypted storage (AES-256)
- Private subnets with no public access
- Automated integrity checks

Data Retention & Disposal

- Configurable data retention based on client requirements
- Secure disposal aligned with SS 714:2025 and ISO 27001 policies
- Automated log rotation and evidence retention for audit purposes

05 Business Continuity & Disaster Recovery

QuickHR uses a resilient architecture designed for high availability and rapid recovery.

High Availability

- Active-active configuration across multiple availability zones
- Redundant compute, network, and storage layers
- Automated failover mechanisms

Disaster Recovery

- Real-time replication to secondary availability zones
- RTO: 4 hours
- RPO: 1 hour
- Quarterly DR drills and restoration testing

Backup Strategy

- Backups are encrypted using AES-256 with integrity validation for secure data recovery.
- Automated restoration testing

06 Subprocessors & Data Residency

QuickHR uses a minimal and carefully managed set of subprocessors. All subprocessors undergo contractual and technical due diligence, including annual reviews.

Primary Subprocessor

QuickHR does not use any additional infrastructure or data-processing subprocessors.

Amazon Web Services — Singapore (ap-southeast-1)

Purpose: Cloud infrastructure, compute, storage

Data Residency: Singapore

Certifications: ISO 27001, SOC 2, PCI DSS

QuickHR does not transfer or store customer data outside Singapore unless explicitly required and contractually approved by the client.

07 Governance, Risk & Compliance (GRC)

Policies & Frameworks

- ISO 27001:2022 ISMS
- PDPA governance framework
- Data Protection Management System (DPMS)
- SS 714:2025 controls
- Risk assessments and DPIAs for all significant changes

Security Operations

- 24/7 Security Monitoring
- Incident response processes with <24h notification commitment
- Monthly internal compliance checks
- Annual external audits

08 Vulnerability Management & Testing

Proactive Security Assurance

- CREST-certified penetration testing, performed annually
- Continuous vulnerability scanning (infrastructure + application)
- Strict patching SLAs
- Automated dependency monitoring for third-party libraries
- Security misconfiguration checks aligned with QHR-UHS 3.0 & AHS 1.0

09 Identity, Access & Privilege Management

- MFA required for all administrators
- RBAC with least-privilege access by default
- Structured and immutable audit trails for every privileged operation
- Quarterly access reviews
- Forced command logging and attribution controls for administrative access

10 Customer Responsibilities & Shared Security Model

QuickHR implements comprehensive security for the platform. Customers are responsible for:

- Managing internal user access
- Maintaining strong password hygiene
- Reviewing audit logs provided
- Setting appropriate retention policies
- Managing employee permissions using RBAC

Full details are available in the Shared Responsibility Matrix upon request.

11 Contact Information

For audit support, compliance documentation, or security reviews:

QuickHR – Security & Compliance Office

Email: security.sg@quickhr.co

Phone: +65 6908 8158

Website: https://www.quickhr.co

Annexure: Compliance & Certification Records

Annex A: ENABLE BUSINESS ISO/IEC 27001:2022

CERTIFICATION INTERNATIONAL

SOCOTEC

CERTIFICATE

No. SCS 102038DIS

certifies that:

Enable Business Pte Ltd

60 Paya Lebar Road #07-38 Office Lobby 2, Paya Lebar Square Singapore 409051

operates a management system that has been assessed as conforming to:

ISO/IEC 27001 : 2022

for the scope of activities:

Provision of cloud-based human resource management system.
Statement of Applicability: Rev 1.0 dated 24 Nov 2023

Issue date: **08 March 2024**
Valid until: **07 March 2027** (Subject to adherence to the agreed ongoing programme, successful endorsement of certification following each audit and compliance with the terms and conditions of certification.)
Original date of certification: **08 March 2021**

Dave CHENG LOON Managing Director

Dave Cheng

Accredited Certification Body SAC ISMS-2019-02

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

SOCOTEC Certification Singapore Pte Ltd
60 Albert Street #13-03, OG Albert Complex
SINGAPORE 189969
www.socotec-certification-international.sg

Annex B: ENABLE BUSINESS MTCS SS584 Level-2 SAAS

CERTIFICATION INTERNATIONAL

SOCOTEC

CERTIFICATE

No. SCS 102038CS

certifies that:

Enable Business Pte Ltd

60 Paya Lebar Road #07-38 Office Lobby 2, Paya Lebar Square Singapore 409051

Data storage same with the address as above

operates a management system that has been assessed as conforming to:

SS584 : 2020

(Level 2 SaaS certification)

for the scope of activities:

Level 2 of Multi-Tier Cloud Security System (MTCS) of Enable Business Pte Ltd located at #07-38, Office Lobby 2, Paya Lebar Square, 60 Paya Lebar Road, Singapore 409051 supporting the provision of cloud-based HR management software services using SaaS model. Applicability and Compensatory Controls SOA Revision 1 dated 18 Mar 2022.

Issue date: **08 March 2024**
Valid until: **07 March 2027** (Subject to adherence to the agreed ongoing programme, successful endorsement of certification following each audit and compliance with the terms and conditions of certification.)
Original date of certification: **08 March 2021**

Dave CHENG LOON Managing Director

Dave Cheng

Accredited Certification Body SAC

MTCS-2016-01

SOCOTEC Certification Singapore Pte Ltd
60 Albert Street #13-03, OG Albert Complex
SINGAPORE 189969
www.socotec-certification-international.sg

Annex C: Data Protection Trustmark

DATA PROTECTION
ASSURED

This certifies that

ENABLE BUSINESS PTE LTD

60 Paya Lebar Rd, #07-38 Paya Lebar Square, Singapore 409051

has been awarded the

Data Protection Trustmark

Certificate Number	Period
DPTM-00172-202306	01/06/2023 – 31/05/2026

Mr Lew Chuen Hong
Chief Executive, IMDA

Certified by:
INFOCOMM MEDIA DEVELOPMENT AUTHORITY

10 Pasir Panjang Road, #03-01,
Mapletree Business City, Singapore 117438

www.imda.gov.sg

Annex D: AWS ISO/ IEC 27001:2013

DocuSign Envelope ID: 3F8FADA4-F0EA-4ADD-9570-343643DC09AB

MGMT. SYS.
RvA C 466

Certificate

CERTIFY POINT
EY

Certificate number: 2013-009

Certified by EY CertifyPoint since: November 18, 2010

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: November 18, 2022
Re-issue date of certificate: November 25, 2022
Expiration date of certificate: October 31, 2025
Last certification cycle expiration date: November 30, 2022

EY CertifyPoint will, according to the certification agreement dated April 1, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

**With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2022.01 dated September 14, 2022, this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.*

DocuSigned by:
Jatin Sehgal
6E3A0F2A5EBF4C7...

J. Sehgal | Director, EY CertifyPoint

Digital version

Annex E: AWS ISO/ IEC 27017:2015

DocuSign Envelope ID: 3F8FADA4-F0EA-4ADD-9570-343643DC09AB

Certificate

Certificate number: 2015-015

Certified by EY CertifyPoint since: October 1, 2015

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO/IEC 27017:2015

Issue date of certificate: November 18, 2022
Re-issue date of certificate: November 25, 2022
Expiration date of certificate: November 30, 2025
Last certification cycle expiration date: November 30, 2022

EY CertifyPoint will, according to the certification agreement dated April 1, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above or the expiration of the corresponding ISO/IEC 27001:2013 certification with certificate number 2013-009.

**With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2022.01 dated September 14, 2022, this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.*

DocuSigned by:
Jatin Sehgal
6E3A0F2A5E8F4C7...

J. Sehgal | Director, EY CertifyPoint

Digital version

Annex F: AWS ISO/ IEC 27018:2019

DocuSign Envelope ID: 3F8FADA4-F0EA-4ADD-9570-343643DC09AB

Certificate

Certificate number: 2015-016
Certified by EY CertifyPoint since: October 1, 2015

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO/IEC 27018:2019

Issue date of certificate: November 18, 2022
Re-issue date of certificate: November 25, 2022
Expiration date of certificate: November 30, 2025
Last certification cycle expiration date: November 30, 2022

EY CertifyPoint will, according to the certification agreement dated April 1, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above or the expiration of the corresponding ISO/IEC 27001:2013 certification with certificate number 2013-009.

**With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2022.01 dated September 14, 2022, this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.*

DocuSigned by:
Jatin Sehgal
6E3A0F2A5EBF4C7...

J. Sehgal | Director, EY CertifyPoint

Page 1 of 6 Digital version

Annex G: AWS ISO/ IEC 9001:2015

DocuSign Envelope ID: 3F8FADA4-F0EA-4ADD-9570-343643DC09AB

MGMT. SYS.
RvA C 466

Certificate

CERTIFY POINT EY

Certificate number: 2014-014
Certified by EY CertifyPoint since: November 4, 2014

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015, the Quality Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO 9001:2015

Issue date of certificate: November 18, 2022
Re-issue date of certificate: November 25, 2022
Expiration date of certificate: November 30, 2025
Last certification cycle expiration date: November 30, 2022

EY CertifyPoint will, according to the certification agreement dated April 1, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

** This certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.*

DocuSigned by:
Jatin Sehgal
6E3A0F2A5EBF4C7...

J. Sehgal | Director, EY CertifyPoint

www.iaf.nu
INTERNATIONAL ACCREDITATION FORUM

Page 1 of 6 Digital version

Annex H: AWS CSA STAR CCM v4.0

DocuSign Envelope ID: 3F8FADA4-F0EA-4ADD-9570-343643DC09AB

CSA STAR CERTIFICATION

Certificate

CERTIFY EY POINT

Certificate number: 2020-026

Certified by EY CertifyPoint since: November 6, 2020

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015, the Cloud Security Management System as defined and implementec by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

CSA STAR CCM v4.0

Issue date of certificate: November 18, 2022
Re-issue date of certificate: November 25, 2022
Expiration date of certificate: November 30, 2025
Last certification cycle expiration date: November 30, 2022

EY CertifyPoint will, according to the certification agreement dated April 1, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above, or the expiration of the corresponding ISO/IEC 27001:2013 certification with certificate number 2013-009.

**With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2022.01 dated October 10, 2022, this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.*

Docusigned by:
Jatin Sehgal
6E3AIF2A5EBF4C7...

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V., located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/regulatory obligations. All rights reserved. © Copyright

Page 1 of 6

Digital version