HR Easily Pte Ltd

# Security Essentials

## An Overview

https://app.hreasily.com

v1.01

# Table of Contents

## Organisational Commitment

The HR Easily management is committed to the continual improvement of the information security of the organisation.

Our practices follow industry-set baselines and best practices. To ensure the reliability and stability of our applications and services, we meet the Center for Internet Security (CIS) benchmark for relevant servers. We follow recommendations from the National Institute of Standards and Technology (NIST) regarding security controls such as cryptography, processes such as change management, or guidelines such as password construction.

Part of our internal exercise to ensure the platform stays resilient and a demonstration of our resolve and credibility to provide a secure solution to the market as we continue our aggressive growth, we annually (at minimum) engage a CREST-certified third party consultant for Penetration testing to subject our public-facing applications against OWASP Top 10 and SANS CWE/25 web application standards. Our mobile application is also subjected to the OWASP Mobile App Security Verification Standard (MASVS).

## Roadmap

We are moving into integrating ISO 27001:2013 controls into our information security processes with a special focus on effective risk management. By implementing these controls, we secure our employee and customer data, we increase resilience to cyber-attacks and reduce the costs associated with information security by eliminating redundancies and streamlining processes.

## Data Handling

Refer to our Privacy Policy (https://app.hreasily.com/privacy-policy) for more details on how HRe handles personal and company information.

## Software as a Service (SaaS) platform

The HR easily application is an all-cloud HR management SaaS platform available in both web and mobile formats (iOS and Android). Users access our services and content through modern web-browsers on an internet-connected desktop or smartphone. We do not maintain any physical servers or storage devices to run our applications. Our services are built on a fully cloud infrastructure provided by AWS within the Singapore region.

We employ redundancy measures to ensure high availability across our platform. This helps us achieve our committed Service Level Agreements (SLAs).

Our service is built on industry-leading platform services which include:

- oAuth for authentication and authorisation
- Chargebee for subscription (billing) management
- Stripe for payment processing

## SaaS Architecture

We are using both multi-tenancy and multi-instance approaches. For white-labelling partnership, the isolation of data and resources that clearly identifies customer data is implemented (multi-instance). Else, only logical (code logic) isolation is implemented across the SaaS platform (multi-tenancy).

## Data Access

**Login**: Users can use the oAuth service provided by Google to sign-up and subsequently login to their account. The traditional username and password credential combination is also available.

User credentials are salted and hashed using SHA-2 and transmitted securely via TLS.

**Two-factor Authentication (2FA)**: 2FA adds an additional layer of security when users login to our application. Industry standards recognise three authentication factor options: (1) something you know like your password, (2) something you have like a smart card, and (3) something you are like a biometric characteristic such as a fingerprint.

We use One-time passwords (OTP) as a second factor. Our OTPs are unique codes that are valid for a single login session for a defined period of time.

- What you know: Password
- What you have: OTP sent via email

**Role-based access control (RBAC)**: RBAC method is used to control access to the system based on the individual user roles. By implementing the RBAC method, it is easier to manage the permission to the user based on the roles and organisation assigned to them. For example, employee data can only be accessed by an assigned administrator with specific roles. [Link]

The allowed roles are  implemented in a whitelisting approach before accessing requested resources.

# Our Infrastructure

## Our Cloud Service Provider (CSP): Amazon Web Services (AWS)

AWS is a leader in Cloud infrastructure and platform as a service (CIPS) since 2010. They regularly undergo independent third-party attestation audits to maintain security and compliance in the cloud. These audit and compliance reports give us the clarity to utilize AWS to host and process highly confidential data. See the list of compliances here: AWS Compliance Programs

**Singapore**: They are the first global cloud service provider to achieve the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584) Level-3 (CSP) certification. [Link]

This provides us with an assurance of their ability to comply with the standards of protection under the Data Protection Provisions of Singapore's Personal Data Protection Act (PDPA).

**Indonesia**: On 4 October 2019, Indonesia's Government Regulation No. 71 on the Organization of Electronic Systems and Transactions (GR 71/2019) clarifies that privately-scoped Electronic System Operators in Indonesia can now transfer or store data offshore. [Link]

This implies that privately-scoped businesses in Indonesia can now be fully confident to engage our services as regulatory limits (GR 82/2012) has been lifted (i.e. GR 71 of 2019 supersedes GR 82 of 2012).

However, some sectors (i.e. the financial sector) are subject to relevant regulations that may impose additional data storage and management requirements, e.g. storing certain types of data onshore in Indonesia. Although these regulations are likely to be reviewed in the light of GR 71, we encourage our customers to discuss with their legal department or to contact us for any clarifications.

*The flexibility, reliability and security of AWS make it an ideal choice for our infrastructure and application needs. The highly secure and resilient infrastructure and services of AWS allow us to make efficient, scalable and cost-effective decisions.*

## System and Network

Our infrastructure is contained within our access-controlled VPCs which provides total isolation. Network segmentation is achieved by dividing our VPCs into public and private subnet layers; the only public-facing listeners are our load balancers which are managed by AWS.

We maintain separate development, staging and production accounts for each layer of our service. Only shared services have access to our staging and production environments. A process is in place for requesting and approving remote connections to servers.

The "least privilege" model ensures that only users who need access in the fulfilment of their duties and responsibilities are granted the appropriate rights and permissions. Privileged access are performed over secure channels ( e.g. over encrypted network connections using SSH)

Activities performed using shared and privileged accounts are monitored. Access control (i.e. security groups, users, roles, and permissions) is reviewed quarterly.

Our static content is delivered through CloudFlare, one of the largest internet services providers that aims at making websites fast, secure, and reliable.

Our public-facing web applications and APIs are also protected by CloudFlare, cloud-based web application and API protection (WAAP) service which provides a combination of distributed denial of service (DDoS) protection, bot mitigation, API protection and a web application firewall (WAF).

We follow the following standards as our server security baselines: NIST Special Publication 800-123: Guide to General Server Security, CIS-20 Controls for Implementation Group 2, and AWS Security Best Practices.

# Data Handling

## Payment processing

We do not store any PCI information in our databases and logs.Payment processing is implemented through Stripe, who holds the customer's payment information such as credit card or bank details. Stripe is PCI Service Provider Level 1- compliant. [Link]

## Data in transit

Data from users to our services are over a secure HTTP (HTTPS) connection and encrypted end-to-end using SHA256 ECDSA for signing and SHA256 RSA for compatibility. We only allow HTTPS connections from visitors supporting TLS v1.2 and above. These protocols offer modern authenticated encryption (also known as AEAD) for added security .

## Data at rest

We follow the recommended cryptographic functions stipulated by NIST in Special Publication 800-175B. SP 800 is a published guidance to the US Federal Government for using cryptography to protect its sensitive but unclassified digitised information during transmission and while in storage.

Data repositories that hold or manage sensitive commercial or personal information are encrypted at rest using AES-256. Our containers (AWS S3 buckets) for logs and database backups are also encrypted by default.

Full disk encryption is also mandatory for all employee laptops and workstations.

## Data retention

We retain data for as long as necessary to fulfil the purposes for which we collected it. This also includes satisfying any legal, accounting, or reporting requirements, to establish or defend legal claims, or for fraud prevention purposes.

Our policies have defined a retention period of one (1) year but not more than seven (7) years. This period allows for analysis and investigations should the need arise.

### What happens to your data if you leave HR easily?

If you terminate or cancel your subscription with us, you can request for a deletion of your account. However, your data from backups and logs will be retained according to our data retention policies.

You may request a copy of your data, but this should be made before requesting for the deletion of your account.

## Data transfer

The clause for the transfer of personal data is stated in the privacy policy for individuals (Clause Nos. 3 and 4).

Data collected and stored on our systems are only accessible by a select number of internal personnel on a need to basis only. The extraction and transferring of data can only be carried out by key personnel and directed through by means of strict approval processes to ensure that the data is duly protected. Unless deemed unnecessary, all data extracted are anonymised, omitted or redacted to protect personal information. For research and analysis purposes, only aggregate information is retrieved, i.e. no personal data is extracted.

It is part of the company's policy to not participate in the leasing or sale of any information, personal or otherwise.

## Data Processing Agreement (DPA)

### Who is a data subject?

*"a natural person from whom personal data is collected, processed and stored."* - GDPR

### Who is a data controller?

*"a natural or legal person, which alone or jointly with others, determines the purposes and means of personal data processing."* - GDPR

For example: a business entity or organisation obtaining customer or employee details

### Who is a data processor?

*"a natural or legal person that processes personal data on behalf of the data controller."* - GDPR

A data processor would be a separate business entity serving the interests and carrying out the instructions of the data controller in its processing of the personal data. The role of a data processor could include storing data, retrieving data, running the payroll for a business, carrying out marketing activities, or providing security for data.

### Where can I find our DPA?

The organisation collecting and using personal data should have a data processing agreement with a data processor. Since we are a data processor, it is up to the organisation, who is the data controller (i.e. the employer / our customer), to have in place and implement a data processing agreement that is compliant.

The data processing agreement (DPA) is our Privacy Policy and Terms and Conditions.

If the data controller wishes some other terms or agreement to apply then it is incumbent upon them to arrange that with us in accordance with their data processing requirements.

## Data Breach Notification

Our infosec policies include a data breach plan included in Clause No. 27 of the Privacy Policy for Individuals. Customers and affected parties will be notified as soon as reasonable. You will be contacted through the company information provided or through the email address provided (for individuals).

# Our Data Protection Policy

*Lawful, fair and transparent processing*

1. To ensure its processing of data is lawful, fair and transparent, HReasily shall maintain a Register of Systems.
2. The Register of Systems shall contain the following:
    a. The data we collect and in what way
    b. How the data are stored and who has access to them
    c. Sharing the data
    d. Purpose for which the data are used
    e. Data retention (removal and archiving)
    f. Lawful purpose
3. The Register of Systems shall be reviewed at least annually.
4. Individuals have the right to access their personal data and any such requests made to the organisation shall be dealt with in a timely manner.
5. Access requests shall be documented.

*Lawful purposes*

6. All data processed by the organisation must be done on one of the following lawful bases: consent, deemed consent (notification, legitimate interest, business improvement and research) , contract, legal obligation, vital interests or public task.
7. Reliance of the organisation in the collection, use and disclosure of personal data for any of the purposes in which the consent is deemed should undergo risk assessment. This assessment shall be documented. When necessary and required by law, reliance on this consent shall be made available to the users.
8. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent, except when it falls under deemed consent by notification, shall be documented.
9. Where communications are sent to individuals based on their consent, the option for the individual to withdraw their consent should be clearly available and systems should be in place to ensure such withdrawal is reflected accurately in the HReasily systems.

*Data minimisation*

10. The organisation shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

*Accuracy*

11. The organisation shall take reasonable steps to ensure personal data is accurate.
12. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

*Data retention*

13. To ensure that personal data is kept for no longer than necessary, the organisation shall put in place a data retention policy for each area in which personal data is processed and review this process annually.
14. The data retention policy shall consider what data should be retained, for how long, and why.

*Security*

15. The organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
16. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
17. When personal data is deleted or anonymised - this should be done safely such that the data is irrecoverable.
18. Appropriate back-up and disaster recovery solutions shall be in place.

*Breach*

19. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the appropriate regulatory body.

# Integrations

Indirect or third party access refers to a situation in which our customer data is viewed or used by a third-party application or custom interface. Authorised third-party integrations have legitimate business cases as part of the company's offering of services such as payroll and staffing services, software, products and support.

Our third-party integrations, such as **Xero**, **Deputy**, and **Enterpryze**, are accessed via our external API.

OAuth tokens or any customer-identifying information are not exposed within our applications nor shared with other parties.

All integrations are accomplished using oAuth v2.0. “Bearer tokens” and not credentials (user and password) are used to authenticate each request. Each request is protected in transit through HTTPS.

# Vulnerability Management

## Preventive maintenance

The most recent and critical security patches must be installed on the system as soon as practical and reasonable. Immediate application of security patches is ideal unless this interferes with business requirements where a reasonable expectation of delay is justified.

Regular preventive maintenance (security and/or system patches) will also be carried out once a month.

## End-point protection

End-point protection is another layer of security protection for our company assets (data and resources) against malicious attacks, ransomware and viruses.

All end-points that are connected to internal networks via remote access technologies or personal workstations (BYOD) that access company resources use the most up-to-date anti-virus software.

## Responsible disclosure

A publicly-available page that outlines how independent security researchers, who understand the severity of the risk, can disclose security vulnerabilities found on our products and services. Our responsible disclosure page is located here.

# Our Workflows: The Agile Environment

## Software development

We adopt the best of agile practices and we continue to improve the way we work by constantly reviewing the way we work.

Agile teams select the amount of work possible to be done based on their availability. Agile iterative development means that the team itself may decide what it is able to do based on their capabilities and experience from the previous iteration.

The Engineering Team runs a very tight ship. Workflows are almost clearly outlined and followed by every single member of the Engineering Team and reviewed almost every month for improvements.

## Software testing

In an Agile environment, the Engineering, Product and Quality Assurance Team, work collaboratively to make improvements on an ongoing basis. We embrace a shared responsibility in ensuring we deliver a high-quality end product and service.

Our software testing processes aim to deliver consistent results through a set of standardised procedures to ensure that the product design does not only meet the requirements and specifications of our customers but is free from bugs, errors, vulnerabilities and other defects.

We minimize the risk of defects while maximizing end-user experience by incorporating software and quality assurance testing throughout our entire engineering process.

Our testing methods utilise both manual and automated processes.

# Risk Management

The core of our information security framework is geared toward managing the risks that affect confidentiality, integrity and availability of our application and services. We follow the ISO 27001 recommendations for risk management.

To determine our set of basic security controls - we follow the 20 prioritised set of actions from the Center for Information Security. CIS-20 collectively form a defence-in-depth set of best practices from security researchers all over the world that mitigate the most common attacks against systems and networks. Thus, CIS-20 provides us with the sufficient basis to kickstart our information security framework.

## Information security policies

The information security framework contains a list of documents and policies that defines our cybersecurity program. These documents are the cornerstone of the information security framework that reflects our security perspective and the management's strategy for securing data and information.

### How do we maintain accuracy in our records and documents?

Information security-related records and documents are protected against unauthorised changes or deletion according to the **Access Control Policy**. Logs and audit trails are immutable and system-generated. Request for access to information follow the **Information Classification and Handling**

## Compliances and certifications

As an organisation, the ISO 27001 compliance is in the roadmap. The Data Protection Trustmark Certification, a.k.a. PDPA Certification is also in the pipeline.