# Information Security Summary for breatheHR

WHAT ARE WE DOING TO PROTECT YOU

## Information Security Management System (ISMS)

breatheHR management is committed to protect the information assets it keeps for our customers, partners and our own information assets and has set objectives for information security management.

- breatheHR operates and maintains an information security management system (ISMS) to control its information assets appropriately. Certification to the information security standard ISO 27001 will be achieved prior to April 2018.
- breatheHR has implemented and applies its internal policies and procedures that support the ISMS. As part of a management system these will be independently audited by a certification body at least annually and by external security specialists.
- breatheHR develops and provides ongoing security awareness for all staff and actively promotes the key principles of information security.
- breatheHR implements human, organisational and technological security controls driven by the ISMS controls (Statement of Applicability) to protect its information assets (including personal data) from unauthorized access, unwanted disclosure, modification, theft / loss, denial of service attacks, or any other threat.
- breatheHR has completed a full company wide information classification assessment, this allows us to understand the data in every part of our business (both our own data and that entrusted to us), the highest level of protection required for each of these data sets and how we can further implement controls to reduce the likelihood of an incident impacting these assets in the future.
- breatheHR uses a formal information security risk management framework to identify and manage known or potential risks to the information assets within our business. Our risk management framework analyses each information asset against the possible loss of confidentiality, integrity and availability and defines appropriate controls.

- breatheHR uses a formal incident management process to identify, contain and recover from a security incident should one occur and uses this process to help prevent reoccurrence.
- breatheHR complies with all legal, regulatory and contractual requirements related to information security and adopts UK law guidelines, industry standards and best practice for information security.
- breatheHR delivers its services based on the following legal / regulatory framework
    - EU General Data Protection Regulations;
    - Telecommunications Act;
    - Contracts with breatheHR customers; and
    - breatheHR utilise third party legal expertise for advice.
- breatheHR uses a scalable cloud computing platform with high availability and dependability.
- To achieve end-to-end security and end-to-end privacy all services are built in accordance with security best practices, privacy by design requirements and appropriate security controls.

## Policy and Procedures

breatheHR has developed policies and procedures based on industry and vendor best practices to protect the information assets it keeps for our customers, partners and our own information assets. The communications and operations management is planned for and deployed with regard to the security of breatheHR information assets and the operations of the whole information processing environment.

Our policy and procedures set standards for our information security controls, some examples being:

- Information security policy
- Clear desk and clear screen policy
- Asset management policy
- Cryptographic policy
- Access control policy
- Acceptable use policy
- Mobile computing policy
- Incident management procedure

- Information classification procedures
- Risk management procedure
- Internal audit procedure
- Document and records control procedure
- Corrective actions procedure
- Preventive actions procedure

Each policy and procedure supports the required controls as set out by the ISO27001 standard Statement of Applicability and how breatheHR manages its information.

## Our Security Officer

Jonathan Richards (jonathan@breathehr.com)

## Our Privacy Policy

For further information on how process (collect, store, share and handle) your data is available in our company privacy policy.

If you have any questions regarding our Privacy Policy, please feel free to contact us.

# Frequently Asked Questions

## Where is my data held?

breatheHR utilises the world's most popular application hosting company, Amazon Web Services (AWS). Specifically, breathe utilises AWS EU-WEST region, with all our databases restricted to their IRELAND location. We have a failover site with AWS in FRANKFURT in Germany. This means we never store your data, or indeed any of our backups, outside the EU.

## How secure is my data?

The security of your data is our number one priority. breatheHR uses HTTPS encryption that ensures your data is always encrypted as it travels from our servers to your web browser. A dedicated access server monitors, logs and controls all access to our servers. It provides a single point of entry and ensures that your data can only be accessed from specific locations that we control. This process uses multiple layers of authentication and any attempt to access our servers from any other location will be denied and logged.

Our servers are held in a highly secure data centres that have complete CCTV coverage, motion sensors, reinforced access doors, controlled key storage systems, and an array of additional physical controls

## How do you ensure I can always access my data?

The platform that runs breathe maintains an average annual uptime of greater than 99.995%. This is achieved by using AWS Elastic Beanstalk load balancing as our primary web technology.

In the unlikely event that the system fails our technical team run monthly exercises to ensure a new environment could be spun up with minimum interruption.

All web and data instances are monitored on a moment by moment basis using industry standard monitoring tools that will alert our technical team should errors occur.

As a final precaution, encrypted AWS RDS snapshots (backups) are taken at approximately midnight daily.

For more detailed information about how we maintain the security and reliability please see Security and Reliability - keeping your data safe.

## Can I get my data out if I decide to leave?

Yes, it is very simple to export your data from the application and your documents can be individually downloaded. If you have any questions just email or call our Support Team.

## Would you sell our data to other companies?

No, given the fact that it is illegal without obtaining your consent to do this, we have no need or desire to sell your data and would never do this.

## Do your systems undergo penetration testing?

Yes, and we view it as a positive thing. The result of the last test demonstrated that our authentication controls are effective at limiting access to authorised users only and could not be bypassed by professional security analysts.