



Security and Reliability

KEEPING YOUR DATA SAFE

Table of Contents

TABLE OF CONTENTS	2
PHYSICAL SECURITY	8
WHERE IS MY DATA HELD?	8
HOW SECURE ARE THE AWS DATA CENTRES?	8
ACCESS IS TIGHTLY CONTROLLED	8
ENTRY IS CONTROLLED AND MONITORED	8
AWS DATA CENTRE WORKERS ARE SCRUTINIZED, TOO	8
MONITORING FOR UNAUTHORIZED ENTRY	9
AWS SECURITY OPERATIONS CENTERS MONITORS GLOBAL SECURITY	9
LAYER-BY-LAYER ACCESS REVIEW	9
MAINTAINING EQUIPMENT IS A PART OF REGULAR OPERATIONS	9
EMERGENCY-READY BACKUP EQUIPMENT	9
TECHNOLOGY AND PEOPLE WORK TOGETHER FOR ADDED SECURITY	10
PREVENTING PHYSICAL AND TECHNOLOGICAL INTRUSION	10
SERVERS AND MEDIA RECEIVE EXACTING ATTENTION	10
THIRD-PARTY AUDITORS VERIFY OUR PROCEDURES AND SYSTEMS	10
AWS CERTIFICATIONS	11
NETWORK SECURITY	11
VPC (VIRTUAL PRIVATE CLOUD)	11
AWS GUARDDUTY	11
ALERTLOGIC INTRUSION DETECTION	12
AWS CONFIG	12
AWS SHIELD	12
DATA SECURITY	13
RDS (RELATIONAL DATABASE SERVICE)	13
BACKUPS	13
DATA ENCRYPTION	13
AWS ACCESS TO NETWORK AND DATA	14
BREATHE EMPLOYEE ACCESS TO NETWORK AND DATA	15
WEB SERVER ACCESS	15
FRONT-END ACCESS	15
DATABASE ACCESS	15
REPORTING / MARKET RESEARCH	15



TECHNICAL ENVIRONMENT SECURITY	16
OPERATING SYSTEMS	16
DEVELOPMENT LANGUAGES AND FRAMEWORKS	16
SSL / TLS	16
USER PASSWORDS – BEST PRACTICE	17
2FA	17
APPLICATION SECURITY	18
SESSION HIJACKING AND SESSION REPLAY ATTACKS.	18
CROSS-SITE REQUEST FORGERY (CSRF) ATTACKS	18
INJECTION ATTACKS	18
CSS INJECTION	18
COOKIE ENCRYPTION	18
PRIVILEGE ESCALATION	19
DDOS ATTACKS	19
OTHER FORMS OF ATTACK AND CONCLUSION	19
PENETRATION TESTING	19
ISO AUDITING	19
HOW SECURITY MAINTAINED THROUGH THE RELEASE CYCLE?	19
DEVELOPER REVIEW	20
PEER REVIEW	20
AUTOMATED TESTING	20
QA AND FRONT END SECURITY REVIEW	20
HOW IS AVAILABILITY ENSURED?	21
A NOTE FROM THE CTO	21
PLATFORM AVAILABILITY	21
FAILOVER	21
MONITORING	21
BACKUP	21
DATA PROTECTION	22
SUMMARY	22
GDPR COMPLIANCE	22
ISO 27001 CERTIFICATION	22
PAYMENT DATA	22
ISO 27001 SECURITY CERTIFICATION	22
FREQUENTLY ASKED QUESTIONS	ERROR! BOOKMARK NOT DEFINED.

Introduction from our CTO

If you are reading this document, then you are serious about security. So am I.

I recognise that Breathe has both a legal and moral responsibility to ensure that we comply with data protection legislation and industry standards. Our company value is to “do the right thing” and that means not just ticking boxes to ensure your data is safe, but questioning everything we do with the intent of making it safer.

It’s not just the right thing to do; it’s good business sense. We survive by ensuring your data is safe. We thrive by constantly looking for ways to make it even safer.

It’s my intent that all common security questions should be answered here. However, I am always delighted to be contacted if you have questions that are not addressed in this document so please do not hesitate to drop me an email at security@breathehr.com.

Gareth Burrows

Chief Technical Officer, Breathe



Physical Security

Where is my data held?

	<p>Breathe utilises the world’s most popular application hosting company, Amazon Web Services (AWS). Specifically, Breathe uses AWS EU-WEST region, with all our databases restricted to their IRELAND location. We have a failover site with AWS in London. This means we never store your data, or indeed any of our backups, outside the EU. Naturally, we keep abreast of changing political landscapes and review this decision regularly.</p>
---	---

How secure are the AWS data centres?

AWS data centre physical security begins at **the Perimeter Layer**. This layer includes a number of security features depending on the location. These include security guards, fencing, security feeds, intrusion detection technology, and other security measures.



The Perimeter Layer.

Access is tightly controlled

AWS restricts physical access to people who need to be at a location for a justified business reason. Employees and vendors who have a need to be present at a data centre must first apply for access and provide a valid business justification. The request is reviewed by specially designated personnel, including an area access manager. If access is granted, it is revoked once necessary work is completed.

Entry is controlled and monitored

Entering the Perimeter Layer is a controlled process. AWS staffs its gates with security officers and employs supervisors who monitor officers and visitors via security cameras. When approved individuals are on site, they are given a badge that requires multi-factor authentication and limits access to pre-approved areas.

AWS data centre workers are scrutinised too

AWS employees who routinely need access to a data centre are given permissions to relevant areas of the facility based on job function. Staff lists are routinely reviewed by an area access

manager to ensure each employee's authorisation is still necessary. If an employee doesn't have an ongoing business need to be at a data centre, they have to go through the visitor process.

[Monitoring for unauthorised entry](#)

AWS are continuously watching for unauthorised entry on their properties, using video surveillance, intrusion detection, and access log monitoring systems. Entrances are secured with devices that sound alarms if a door is forced or held open.

[AWS security operations centres monitors global security](#)

AWS Security Operations Centres are located around the world and are responsible for monitoring, triaging, and executing security programs for their data centres. They oversee physical access management and intrusion detection response while also providing global, 24/7 support to the on-site data centre security teams



The Infrastructure Layer

The **Infrastructure Layer** is the data centre building and the equipment and systems that keep it running. Components like back-up power equipment, the HVAC system, and fire suppression equipment are all part of the Infrastructure Layer.

[Layer-by-layer access review](#)

Like other layers, access to the Infrastructure Layer is restricted based on business need. By implementing a layer-by-layer access review, the right to enter every layer is not granted by default. Access to any particular layer is only granted if there is a specific need.

[Maintaining equipment is a part of regular operations](#)

AWS teams run diagnostics on machines, networks, and backup equipment to ensure they're in working order now and in an emergency. Routine maintenance checks on data centre equipment and utilities are part of regular operations.

[Emergency-ready backup equipment](#)

Water, power, telecommunications, and internet connectivity are designed with redundancy, so we can maintain continuous operations in an emergency. Electrical power systems are designed to be fully redundant so that in the event of a disruption, uninterruptible power supply units can be engaged for certain functions, while generators can provide backup power for the entire facility. People and systems monitor and control the temperature and humidity to prevent overheating, further reducing possible service outages.



The **Data Layer**

The **Data Layer** is the most critical point of protection because it is the only area that holds customer data. Protection begins by restricting access and maintaining a separation of privilege for each layer. In addition, we deploy threat detection devices and system protocols, further safeguarding this layer.

Technology and people work together for added security

There are mandatory procedures to obtain authorisation to enter the Data Layer. This includes review and approval of a person's access application by authorized individuals. Meanwhile, threat and electronic intrusion detection systems monitor and automatically trigger alerts of identified threats or suspicious activity. For example, if a door is held or forced open an alarm is triggered. We deploy security cameras and retain footage in alignment with legal and compliance requirements.

Preventing physical and technological intrusion

Access points to server rooms are fortified with electronic control devices that require multi-factor authorisation. We're also prepared to prevent technological intrusion. AWS servers can warn employees of any attempts to remove data. In the unlikely event of a breach, the server is automatically disabled.

Servers and media receive exacting attention

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycle. We have exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

Third-party auditors verify our procedures and systems

AWS is audited by external auditors on more than 2,600 requirements throughout the year. When third-party auditors inspect our data centre they do a deep dive to confirm we're following established rules needed to obtain our security certifications. Depending on the compliance programme and its requirements, external auditors may interview AWS employees about how they handle and dispose of media. Auditors may also watch security camera feeds and observe entrances and hallways throughout a data centre. And they often examine equipment such as our electronic access control devices and security cameras.

AWS Certifications

AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, and 27018:2014. These certifications are performed by independent third-party auditors. Our compliance with these internationally-recognised standards and code of practice is evidence of our commitment to information security at every level of our organization, and that the AWS security programme is in accordance with industry leading best practices.

Network Security

VPC (Virtual Private Cloud)



An Amazon VPC is a logically isolated portion of Amazon Web Services that gives us a virtual network where you can launch instances with particular rules and policies to get access to the Internet. It is really like having a virtual network inside a cloud computing service with the possibility to have a specific range of IPs, subnets and networks rules in order to specify a set of rules to communicate with external resources – such as Breathe users.

Using a VPC means we can

1. Lock down the type of traffic allowed through to Breathe resources
2. Utilise Network access control lists (ACLs) to act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level
3. Capture and log information about the IP traffic going to and from Breathe resources

AWS GuardDuty



Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorised behaviour to protect your AWS accounts and workloads. an intelligent and cost-effective option for continuous threat detection in the AWS Cloud. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritise potential threats. GuardDuty analyses tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs.

Alertlogic Intrusion Detection



Whilst AWS GuardDuty is an inexpensive and easy to use solution, the nature of our clients' data resulted in Breathe electing to add a more comprehensive solution for Intrusion Detection. AlertLogic provides a fully managed service to detect a wide array of attack methods for security threats lurking in our network traffic, including exploits in web app frameworks, containers, app stack components, and OWASP Top 10. It also provides vulnerability and security configuration management to identify vulnerabilities hidden at all layers of our application stack, and a Threat Risk Index to assess our security posture. 24/7 coverage and expert incident analysis and live notifications of active attacks in 15 minutes mean that Breathe never sleeps when it comes to protecting our clients' information.

AWS Config



AWS Config is a service that enables us to assess, audit, and evaluate the configurations of our AWS resources. Config continuously monitors and records our AWS resource configurations and allows us to automate the evaluation of recorded configurations against desired configurations. Config allows us to maintain a history of configuration changes for auditing purposes, ensure that our current configuration matches our desired configuration for security consistency, and ensure compliance with industry best practice.

AWS Shield



AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimise application downtime and latency. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target web sites or applications.

Data Security

RDS (relational database service)



Breathe uses AWS RDS with a MySQL database to store all client data, and also for all business reporting needs. As well as a production environment, we maintain a staging environment for deployment purposes, as well as test environments for development and research purposes. Only the production environment contains real world client data. All databases are encrypted at rest using RDS supplied keys, and traffic to the database instances is restricted to the Breathe web service, so it cannot be directly attacked by malicious parties – it can only be accessed by resources in the Breathe Virtual Private Cloud. The security group used for the production database is used ONLY for that purpose and references no other resources

Backups



Breathe uses a multi-faceted approach to backup solutions, with two independent solutions taking backups nightly for 5 days. One of these solutions utilises RDS snapshots, taking encrypted backups once a day. The second solution is proprietary to be used only in a complete failure of AWS, and encrypts a backup using a 1024 bit key before storing it in an encrypted and private AWS S3 storage bucket. Only the company CTO and the code performing the backup have access to this storage bucket, and obsolete files are rotated out automatically every night. Backups exist for business continuity in the case of a complete failure of the database or inability to access it. Partial, granular or account specific restorations are not possible.

Data Encryption



Whilst the majority of the data is encrypted at rest, protecting the data from physical theft, critical information such as system security data and user passwords are also encrypted at all times within the database. The passwords are encrypted using a salted hash. Hash algorithms take a chunk of data (e.g., your user's password) and create a "digital fingerprint," or hash, of it. Because this process is not reversible, there's no way to go from the hash back to the password. To prevent malicious users running lists of possible passwords through the same algorithm and then looking up the passwords by their hash a small chunk of random data -- called a salt – is added to the password before it's hashed. Finally, the processing method of salt and hash is designed to be computationally expensive, which makes it impractical to use even giant processing solutions to hack Breathe passwords.

AWS access to network and data

Amazon state categorically in their privacy documentation (<https://aws.amazon.com/compliance/data-privacy-faq/>) that:

“We do not access or use your content for any purpose without your consent. We never use your content or derive information from it for marketing or advertising.”

In addition they also state:

“We do not disclose customer information unless we're required to do so to comply with a legally valid and binding order. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing content information.”

The AWS Production network is segregated from the Amazon Corporate network and requires a separate set of credentials for logical access. The AWS Production network requires SSH public-key authentication through a bastion host.

AWS developers and administrators on the Amazon Corporate network who need to access AWS cloud components must explicitly request access through the AWS access management system. All requests are reviewed and approved by the appropriate owner or manager.

User accounts are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated in Amazon's Human Resources system. Windows and UNIX accounts are disabled and Amazon's permission management system removes the user from all systems.

Breathe understands and accepts the ramifications of the AWS shared responsibility model.

Breathe employee access to network and data

Web server access

The Breathe web servers are only accessible by breathe developers using SSH connection. Each access attempt is centrally logged. Server instances are rotated out every 24 hours to prevent brute force attacks and repeated attempts using incorrect credentials generate an alarm and lockout. Policies exist to replace access keys in the event of employees leaving or assets being misplaced. Access is restricted by IP address to the Breathe offices and by policy to authorised staff.

Front-end access

Access to client data through the front end of the application is restricted to support personnel who have obtained positive permission (in the form of a tick box) from the client. Permission is granted through an administrative tool requiring two factor authentication, and each access / access attempt is centrally logged. Access is restricted by IP address to the Breathe offices and by policy to authorised staff.

Database access

Database access is given to 3rd line support and development personnel in order to research support issues that require close examination or correction of the data. Access is programmatic in nature and restricted by policy to accounts that have given active permission for Breathe staff to work on their data. Access is restricted by IP address to the Breathe offices and by policy to authorised staff.

Reporting / Market Research

Aggregated data is used for the purpose of reporting on use of the application, and optimising performance, as well as research into the success of features. This data is automatically redacted before being exported to a separate Business Intelligence system (Microsoft Power BI). The BI tool has no access to unredacted client employee data.

Technical Environment Security

Operating Systems



The Amazon Linux AMI is a supported and maintained Linux image provided by Amazon Web Services for use on Amazon Elastic Compute Cloud (Amazon EC2). It is designed to provide a stable, secure, and high-performance execution environment for applications running on Amazon EC2. Amazon Web Services provides ongoing security and maintenance updates to all instances running the Amazon Linux AMI. The configuration of the Amazon Linux AMI enhances security by focusing on two main security goals: limiting access and reducing software vulnerabilities. The Amazon Linux AMI limits remote access capabilities by using SSH key pairs and by disabling remote root login. Additionally, the Amazon Linux AMI reduces the number of non-critical packages which are installed on your instance, limiting your exposure to potential security vulnerabilities. Security updates rated "critical" or "important" are automatically applied on the initial boot of the AMI.

Development Languages and Frameworks



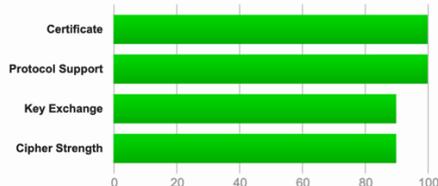
Breathe has been written primarily in Ruby on Rails. Additional web technologies have been implemented where necessary. It is Breathe policy that all technology platforms remain on supported versions, to ensure we can apply the latest security updates. All updates are applied to staging environments before being approved for the production environment. For a fuller examination of the Breathe technology stack, we recommend usage of the site <https://builtwith.com>

SSL / TLS



Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic security protocols. They are used to make sure that network communication is secure. Their main goals are to provide data integrity and communication privacy. The SSL protocol was the first protocol designed for this purpose and TLS is its successor. SSL/TLS protocols allow the connection between two mediums (client-server) to be encrypted using a cipher. As of June 2019 the only version of TLS supported by Breathe is 1.2. We do not support anything older. The signature algorithm used by the Breathe application is SHA256withRSA with a 2048 bit key. Our configuration permits us a score of A at <https://www.ssllabs.com>, and it is our intention for us to maintain that score.

Overall Rating



User passwords – best practice.

NIST Breathe clients are allowed to set their own passwords, with the requirements they have a minimum length of 6 characters. The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce and produces a set of password recommendations largely considered the industry standard. The most recent recommendations to your users in keeping their accounts secure are to;

Remove periodic password change requirements

There have been multiple studies that have shown requiring frequent password changes to actually be counterproductive to good password security, but industry has doggedly held on to the practice.

Drop the algorithmic complexity

No more arbitrary password complexity requirements needing mixtures of upper-case letters, symbols and numbers. Like frequent password changes, it's been shown repeatedly that these types of restrictions often result in worse passwords.

Increase length of password

Whilst password complexity and the requirement to change passwords have been shown to be counterproductive, the one factor that remains constant in the guidelines is password length. NIST recommend a minimum password length of 8 characters. A passphrase of 12 or more characters is the Breathe recommendation.

The full NIST guidelines (2017) are available from <https://pages.nist.gov/800-63-3/sp800-63b.html>

2FA

Breathe does not currently offer a 2FA solution for end users, although it has been implemented in the system administration tools. This is something we are considering for the product roadmap.

Application Security

Session hijacking and session replay attacks.

Company and employee information is not stored in user cookies or session stores. The session is encrypted before being stored in a cookie. This prevents the user from accessing and tampering with content of the cookie. The encryption is done using a server-side secret key accessible only by the breathe developers. Sessions are deleted on logout and reset on login to prevent session fixation attacks.

Cross-Site Request Forgery (CSRF) attacks

To protect against forged requests, we introduce a required security token that our site knows but other sites don't know. We include the security token in requests and verify it on the server. In addition the application adheres to the Restful request model where possible. We also include an unobtrusive scripting adapter, which adds a header called X-CSRF-Token with the security token on every non-GET Ajax call.

Injection attacks.

SQL injection attacks aim at influencing database queries by manipulating web application parameters. A popular goal of SQL injection attacks is to bypass authorisation. Another goal is to carry out data manipulation or reading arbitrary data to prevent this, breathe developers adhere to the following principles.

- Avoid using client-side form data directly in SQL statements server-side
- Sanitise all user input to prevent injection of invalid data or executable code
- Scope all executed code to the specific user to prevent privilege escalation
- Cross-site scripting (XSS) attacks

XSS attacks are the most widespread, and one of the most devastating security vulnerabilities in web applications is XSS. This malicious attack injects client-side executable code. There are two key principles to fend off XSS attacks – Whitelists Input filtering and output escaping, both of which are principles followed by the breathe development team.

CSS Injection

CSS Injection is explained best by the well-known MySpace Samy worm. This worm automatically sent a friend request to Samy (the attacker) simply by visiting his profile. Within several hours he had over 1 million friend requests, which created so much traffic that MySpace went offline. CSS Injection is actually JavaScript injection. This form of attack is prevented in breathe by simply preventing breathe users from styling the application.

Cookie encryption

As of Rails 5.2, encrypted cookies and sessions are protected using AES GCM encryption. This form of encryption is a type of Authenticated Encryption and couples authentication and encryption in single step while also producing shorter ciphertexts as compared to other algorithms previously used. The key for cookies encrypted with AES GCM are derived using a salt value generated from a complex secret.

Privilege escalation

To avoid users in the front end from manipulating forms and/or urls in order to see or edit records they should not be able to see, all searches in the code are scoped to the current employee, meaning that even if a url is manipulated in the front end, the server side code will validate privileges before returning a result.

DDOS Attacks

The fundamental design of the breathe infrastructure makes it inherently resistant to DDOS attacks. The ability to scale up instantly means that most DDOS attack techniques can simply be out scaled until the problem has been neutralised. In addition, the fact that web servers can be rotated out in less than 60 seconds means long term IP based attacks are largely irrelevant. On top of this we utilise AWS web shield to combat common DDOS attacks such as SYN floods and UDP reflection attacks.

Other forms of attack and conclusion

Breathe developers consider header injection, command line injection, unsafe query generation, and many other forms of attack. It is not the intent of this document to outline in detail our approach to security, or indeed to provide a hacker's manual. If you have further specific questions regarding application security please do not hesitate to call.

Penetration Testing



Breathe security is tested externally twice yearly with a penetration test conducted by The Security Bureau of Brighton. This test lasts for a week and comprises a comprehensive examination of both infrastructure and application security using both automated tools and manual techniques.

The test is conducted by CREST accredited consultants and results in an action plan which is then actioned as a priority. We do not share the details of each penetration test.

ISO auditing



Breathe is examined by an independent ISO27001 auditor on an annual basis to ensure that we are following up on identified vulnerabilities and adhering to the standards outlined in our ISO Information Security

Management System (ISMS). All issues identified in the penetration test are logged for discussion by our internal ISO team and resulting actions logged. Our ISO certificate is visible at <https://www.breathehr.com/hubfs/website/security/BreatheHR%20-%20QMS%20ISO27001%20Certificate.pdf>

How is security maintained through the release cycle?

To ensure new code does not degrade the security of the application, it follows a standard procedure before being committed to the production system.

Developer Review

All developers are held accountable for the security of their own code and are thus required to sign off any code they commit from a perspective of security. All developers are also required to attend annual information security training as part of our ISO27001 certification.

Peer Review

No code commits are permitted without a peer review. Code cannot be added directly to the production branch without CTO oversight. Peer review of code includes a security check, which is then randomly checked during internal and external ISO27001 auditing.

Automated testing

As part of our development process, security tests are written alongside new code. These tests are automatically executed during the peer review process and must pass before code can be merged into the main codebase.

QA and front end security review

Code that passes automated testing and peer review is then assessed by our QA team from a perspective of functionality and security. This assessment is conducted in a secure staging environment before being authorised for release.

How is availability ensured?

A note from the CTO

Breathe makes every effort to ensure continuity of service. However, please note that my priority is the security of our clients' data, not the availability of the service. In the event of any outage, my team's priority before even beginning an investigation is to ensure all data is completely secured and under Breathe control.

Platform availability

Breathe maintains superb availability, with an average annual uptime of greater than 99.95%. This is achieved by utilising an AWS Elastic Beanstalk load-balancing, auto-scaling solution as our primary web technology. AWS Elastic Beanstalk is an orchestration service offered from Amazon Web Services for deploying infrastructure which orchestrates various AWS services, including EC2, S3, Simple Notification Service (SNS), CloudWatch, auto scaling, and Elastic Load Balancers. It means Breathe can spin up as many server instances are necessary during busy times to ensure availability, and then switch them off during quiet times to optimise financial efficiency.

Failover

Monthly exercises are run by the technical team to ensure a new environment could be spun up in the event of a complete failure of an AWS availability zone, or even an entire AWS region. Regular business continuity exercises mock-up different scenarios to test the effectiveness of the business to respond to the unexpected. AWS Regions exist all over Europe so the solution is recoverable in all scenarios excepting a major global outage. In the event of a global AWS outage, a backup is kept outside AWS resources, so another cloud platform could be spun up. Our database solution (RDS) is replicated in a different AWS availability zone with automatic failover, meaning if the production database suddenly became unavailable the system automatically switches to the reserve database. This process typically takes less than 30 seconds.

Monitoring

All web and data instances are monitored on a moment to moment basis using industry leader NewRelic Application Performance Monitoring, with automated alarms and alerts set to trigger if the application goes down for more than 60 seconds, or server resources reach a point where they need to be scaled up.

Backup

Encrypted AWS RDS snapshots are taken at approximately midnight daily (AWS provide a 30-minute window in which they run the backup). Backups are kept for 10 days. We maintain a point in time backup / restoration solution which means we can backup to any point in the retention window. Backups are proprietary to AWS and cannot be downloaded, making them extremely secure.



Data Protection

Summary

We are registered with the Information Commissioner's Office (ICO) for the purpose of handling your confidential data within the UK. Strict data handling procedures ensure our staff don't have visibility of passwords and access beyond their ability to support your system. We do not undertake any work involving your data without your permission and hold no responsibility for the maintenance and content of your data.

Our internal processes are regularly audited in line with current legislation and the breatheHR terms and conditions.

GDPR Compliance

At breathe, we have always taken data security and privacy extremely seriously and believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights. As such we are committed to GDPR compliance. For more information see '[Our approach to GDPR compliance](#)'

ISO 27001 certification

At breathe, we have always taken data security and privacy extremely seriously and believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights. As such we are committed to GDPR compliance. For more information see '[Our approach to GDPR compliance](#)'

Payment data

For our credit card payments we use Stripe Payments gateway. Stripe are certified as a Level 1 PCI provider, the highest possible certification level. No card numbers are stored on Breathe resources. In addition our merchant bank requires us to partake in regular reviews of our PCI DSS compliance status to further protect your card data. For more information on stripe security please refer to <https://stripe.com/docs/security/stripe>

ISO 27001 Security Certification



ISO/IEC 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidance. This widely-recognised international security standard specifies that Breathe does the

following:

1. Systematically evaluate our information security risks, taking into account the impact of threats and vulnerabilities.
2. Design and implement a comprehensive suite of information security controls and other forms of risk management to address customer and architecture security risks.
3. Possess an overarching management process to ensure that the information security controls meet our needs on an ongoing basis.

Further information

We hope that this document has answered most of your questions. We have provided the following links for any further information.

Our ICO registration can be viewed at

<https://ico.org.uk/ESDWebPages/Entry/Z7376419>

Our ISO27001 certificate can be viewed at

<https://www.breathehr.com/hubfs/website/security/BreatheHR%20-%20QMS%20ISO27001%20Certificate.pdf>

Our thoughts on the impact of Brexit on Breathe can be viewed at

[https://cdn2.hubspot.net/hubfs/483440/website/security/Brexit%20FAQs%20for%20Website%20Feb_2019%20\(1\).pdf](https://cdn2.hubspot.net/hubfs/483440/website/security/Brexit%20FAQs%20for%20Website%20Feb_2019%20(1).pdf)

Current and historical uptime indicators for Breathe are available at

<http://status.breathehr.com/>