mindful™

Security at Mindful

Version 1.0 March 2020

Reviewed April 20, 2022

mindful™

Table of Contents

Introduction

Mindful's mission is to enable people to get the help they need, from the brands they love, on the terms they choose. To do that, we need to make your data secure, and protecting it is one of our most important responsibilities. We're committed to transparency around our security practices and helping you understand our approach.

mindful

Organizational Security

Network Operations & Infrastructure Security

Security is vital to our networks and infrastructure. Mindful's operational and data networks implement the latest security technologies to ensure security and integrity. Mindful adheres to the following processes and deployment strategies to protect systems and maintain continued operation.

- Mindful's platforms are hosted with Amazon Web Services (AWS), a leading and respected data center provider. Access is strictly controlled and monitored. Datacenter partners are SOC 2 and ISO 27001 certified and provide N+1 redundancy to all electrical power, network services, and HVAC services.
- Mindful's internal network and infrastructure management systems constantly monitor traffic patterns, vulnerabilities, system performance, authentication, access requests, application/security logs, and data flows.
- Mindful uses a combination of automated logging and reporting systems with human oversight and investigation to confirm that our security controls are functioning as designed. Additional controls such as automated anomalous behavior and threat detection tools are implemented to bolster Mindful's security posture.
- Mindful databases, application servers, web servers, and back-end support services maintain multiple failover instances to prevent outages due to single points of failure.
- Mindful performs vulnerability and penetration tests utilizing credentialed and validated 3rd parties followed by peer review and mitigation.
- Hosted data center facilities within AWS provide uptime at that of tier 4 rated facilities according to service levels provided by Amazon, utilizing their resilient design principles.
- Mindful uses a fully automated infrastructure. Server infrastructure is designed with rapid provisioning and de-provisioning principles to appropriately respond to customer needs.
- The rapid patch management process ensures latest security updates are applied in a timely manner. Patching is handled by deploying new server instances with the most up-to-date patches and de-provisioning out-of-date servers.
- Mindful keeps development, test, and production environments logically separated, with a comprehensive change management process used to approve changes before they are deployed to the production platform.

Physical Access Management

Mindful maintains rigorous process and people management to comply with physical security standards protecting our clients and their data against unauthorized access. Below is a list of summary items Mindful implements to provide physical access management.

- Mandatory employee post-offer pre-employment background checks
- Pre-employment social security number trace and criminal database searches
- Mandatory security awareness training with annual renewal training
- Compartmentalized employee access to specific data, applications, servers, environments, or infrastructure elements according to a least privileged methodology
- Equipment and devices are information security classified and delegated to designated personnel who are assigned access-level credentials consistent with the employee's role
- Routine record maintenance of designated employee identity, assigned devices, and respective access rules
- Upon change of employee status, a formal process enacts access termination and/or removal to prevent unauthorized access to our devices and systems
- Mindful's cloud-based production systems do not have any physical dependencies hosted by Mindful. Mindful inherits its physical and environmental controls from the AWS Shared Responsibility Model.

mindful

Protecting Customer Data

Data Security

Mindful is a data processor on behalf of our clients who procure Mindful products and services. Mindful only processes data collected through our products and services when requested by our clients. Data processing by Mindful, including that of PII, is limited by default. Mindful discloses to our client's data processing which may occur during the operation of our solutions, as well as optional configurations to limit such data.

- Client data at rest within Mindful applications and products is encrypted using industry-recognized and approved ciphers and reviewed on an ongoing basis for compliance.
- Purge and persistence of data at rest in Mindful solutions provide multiple methods for Mindful clients to determine how to handle data within Mindful products and services.
- Mindful does not sell or otherwise transfer PII data to any third party.

Product and Application Security

Mindful maintains industry best practices for solution development, testing, quality assessment, and elevation to production environments. With a mature product life cycle, Mindful adheres to product and application security practices summarized below.

- Mindful quality code review and deployment processes are rigorously followed. Automated static code analysis and human review ensure development best practices are implemented across code elevations.
- Mindful operations strictly control the deployment of code and infrastructure updates. All code and infrastructure are deployed via automation following approval processes.
- Mindful maintains advanced logging, alerting, and aggregation tools to provide instantaneous and reliable anomaly alerting.
- Mindful utilizes industry-approved security protocols and encryption mechanisms for data at rest and in transit, such as TLS, HTTPS, PKI, and AES. More information about each use within Mindful solutions is available upon request.

Incident & Disaster Response

Mindful maintains our network integrity, our ability to access systems, and the stable delivery of our products and services in the event of major incidents. Mindful has taken appropriate measures and precautions with our business systems allowing continued operation and management of the Mindful organization.

Mindful maintains annual review and adherence to a formal Incident & Disaster Response Plan.

The primary focus of the plan is:

1. To keep employees safe and able to support the ongoing operation of the business
2. To keep our client's data safe and solutions operational, supporting their business

Conclusion

Here at Mindful, we have a foundational interest in protecting your data. Every person, team, and organization deserves and expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our clients, and we continue to work hard to maintain that trust. Don't hesitate to contact your Mindful Client Success Manager with any questions or concerns.