OnBoard

Security at OnBoard Meetings

Table of Contents

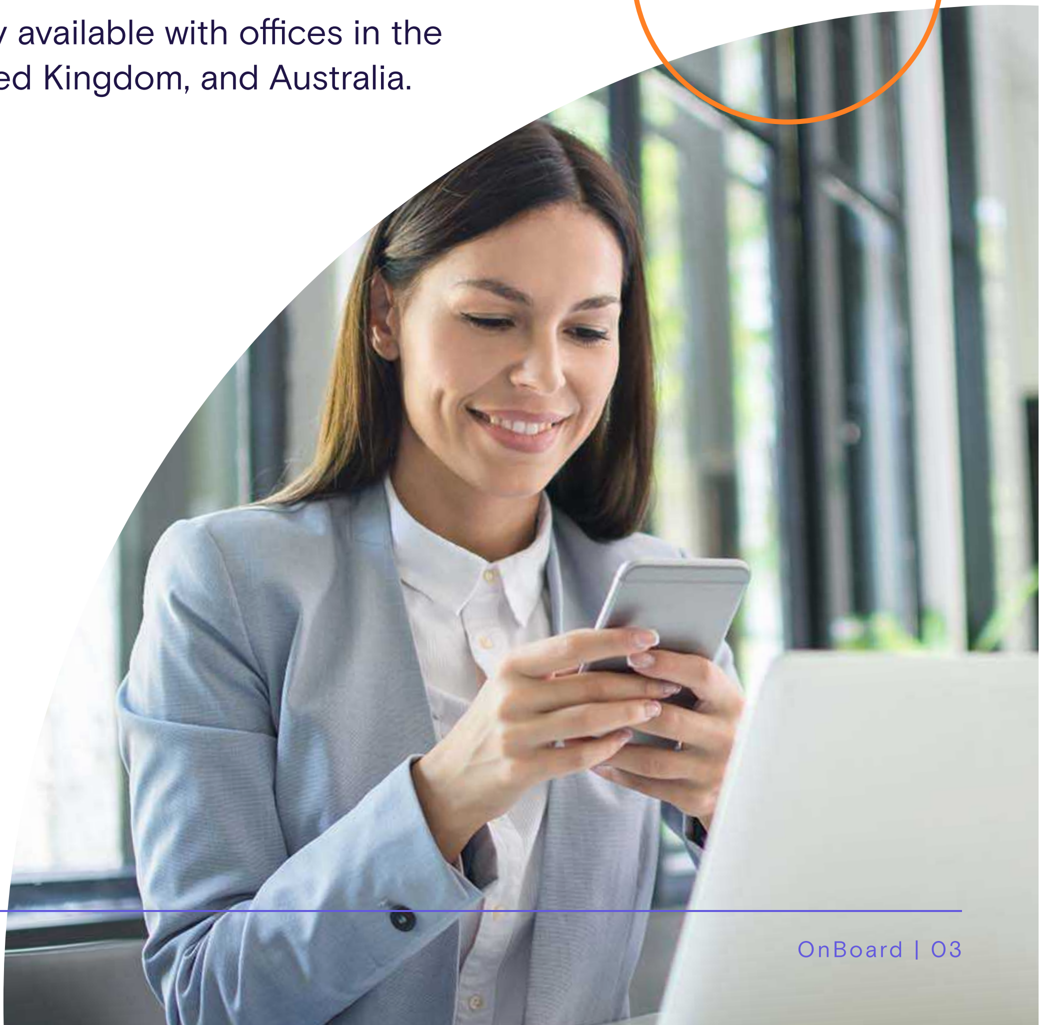
OnBoard Overview

OnBoard is an intelligent Board Management platform that gives board leaders a sophisticated solution to enhance governance, improve decision-making, and uncover key insights by providing a platform that hosts Board Book Builder, Agenda Builder, Voting and Approvals, Automated surveys and questionnaires, meeting analytics and user messaging.

OnBoard is available across multiple platforms, including web, iOS, Android, Windows Store, and the Amazon Store. Key to OnBoard's product experience, the application is fully hosted in the Microsoft Azure cloud which delivers real-time collaboration and decisions, data security, and geo-replicated backups.

OnBoard was built to empowering leaders and teams globally. No matter where you or your organization are today, OnBoard is designed to elevate what's possible for you to achieve.

OnBoard is globally available with offices in the United States, United Kingdom, and Australia.



Security Culture

Security Program

OnBoard maintains an Information Security Management System and this program's key goal is to protect the confidentiality, availability, and integrity of the OnBoard application and data of our customers.

This program is spread out into various section's including Access Management, Incident Response, Business and Continuity Planning, Disaster Recovery Planning, Change Management Program, and a Risk Management Program, and others. Our Security Policies and Procedures are updated at least on an annual basis.

To increase OnBoard's security transparency, we have created a dedicated Trust Center for prospects and customers to be able to view an overview of our security and privacy posture. Our Trust Center also contains a secure resource section which contains various documents including our ISO 27001 Certificate, SOC 2 Type 2 Report, Business Continuity Plan, Incident Response Plan, Secure Agile SDLC, and many others. To access our secure resource section, please contact us via our Contact Page, contact your sales representative, or your customer success manager.

Employee Security

Onboarding/Offboarding

OnBoard maintains a strict set of standards that employees must comply with, prior to employment, to ensure that we are gaining the most qualified individuals for our product. As part of OnBoard's employment process, prior to employment, candidates are required to pass a criminal background check and must sign and comply with our code of conduct, acceptable use policies, and a non-disclosure agreement.

Should an employee resign from the company, user access is immediately revoked to all company resources and company assets are recovered as soon as possible.

Employee Security Training

As part of our ISMS and Cyber Security Training Program, all OnBoard employees are required to go through various cyber training exercises and awareness trainings. These items are conducted on a predetermined schedule in order to ensure our employees remain vigilant for current and emerging cybersecurity threats and attack vectors.

Employee Non-Compliance

Employees that are not in compliance with our policies are subject to disciplinary actions up to and including termination.

Indentity and Access Management

Authentication Methods

When deploying OnBoard, you can decide which authentication method you would like to use. OnBoard supports email, password, and Single-Sign On authentication methods from Google, Microsoft, Okta, and OneLogin.

Single-Sign On (SSO)

OnBoard provides SSO options from Google, Microsoft, Okta, and OneLogin so that your company can choose which option best suites your needs. OnBoard recommends enforcing a Single-Sign On method for your organization to provide more security for users.

Two-Factor Authentication (2FA)

OnBoard also provides 2FA and recommends it be implemented to add another layer of security for users. 2FA is available on an individual level or can be enforced for the entire organization by the organization's administrator.

Granular User Permissions

OnBoard utilizes Granular Permissions, in lieu of a Role Based Access Control method, which enforces individual document and communication permissions. This means that every item in a board book can have its permissions specifically established to ensure that only the intended audience has viewing access. User viewing access can be dictated based on a group and/or down to specific users.

Data Protections

Hosting Platform

OnBoard is completely hosted on Microsoft Azure.
All customer instances within the OnBoard application are logically separated to ensure secure isolation of each customer's data. OnBoard is available to be hosted in one of the following regions: US, UK, Canada, EU, and Australia.

Due to our hosting strategy, access to our systems within Azure are protected in several ways including Active Directory Authentication, MFA verification and our entire platform is structured on a model of least privilege access. In addition, our security team performs access reviews at least twice a year to ensure proper access is preserved according to our policies.

Endpoint Security

Although OnBoard is entirely hosted on Azure, employees still utilize company devices to provide our services. OnBoard does not store any customer data on company workstations, laptops, or removable media. All customer data is safely stored in the production environment.

Company devices are tightly monitored and managed through the duration of their lifecycle. These controls include but are not limited to:

- Mobile Device Management Program
- Configured anti-malware/anti-virus that is auto updated
- Device encryption
- Strong user password enforcement
- Screen lockout policies
- Software installation restrictions
- Company operation-only restrictions
- Secure remote wipe technology
- Proper device wiping and destruction upon withdrawal from the operational lifecycle

Encryption

OnBoard provides encryption to protect user data throughout its lifecycle and has implemented the following technologies to ensure the confidentiality of customer data.

- Data in Transit – When data is transmitted between customers or the OnBoard application, it is protected using TLS 1.2 or higher. .
- Data at Rest – Data at Rest within OnBoard's systems is encrypted with AES-256 encryption technology.

Data Retention and Disposal

Data within the OnBoard application is retained indefinitely, unless a user performs deletions within their instance of the application, or if customer terminates their contract with OnBoard. OnBoard messaging services do provide users with the ability to set retention settings for their messages to allow for their deletion after a specified period of time.

If a customer wishes to terminate their contract, they will have 30 days to collect their data from within the application before it is designated for deletion.

Data Backups

OnBoard maintains a level of high availability from its backups and geo-replication of data - ensuring that data can be restored if necessary.

Vendor Risk Management

Before contracting with any third-party vendor, OnBoard performs a security evaluation regarding the company's security and privacy maturity posture to ensure that their maturity levels are in alignment with the services that we provide and also execute an agreement outlining the applicable obligations and restrictions.

Should OnBoard halt using the vendor, we ensure that all sensitive information is properly collected or destroyed within predefined timeframes.

OnBoard vendors do not have access to any customer Posted Content. OnBoard does not utilize sub-processors for the application.

Change Management

OnBoard maintains formal Change Management and Secure Agile SDLC Policies which ensure that all development, patching, and bug remediation abide by our established processes. This ensures that all system changes are thoroughly tested and approved prior to their implementation to our production environments.

Changes are initiated by product managers, who would like to make an improvement to the OnBoard application or services. All changes are tracked and stored in a version control system which require Quality Assurance (QA) to perform testing, including but not limited to, Test-Driven Development/Behavior-Driven Development, Automated Functional/System and Behavior Testing, automated and manual code review. Once changes are properly reviewed and obtain the required approvals, they will be implemented at the earliest timeframe.

OnBoard's SDLC requires developers adhere to certain security standards and guidelines, including OWASP's Top 10 Application Security Risks, so that they can maintain constant diligence in avoiding web application security risks.

OnBoard makes our Secure Agile SDLC documentation available within our Trust Centers Secure Resource section.

Incident Management, Business Continuity, and Disaster Recovery

Incident Management

OnBoard has developed and follows a formal Incident Response Plan which addresses any availability, integrity, security, privacy, and/or confidentiality issues. Our response plan encompasses the following phases and is carried out by trained professionals:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

If OnBoard encounters a security incident, we will notify the affected users without undue delay of us becoming aware of the incident. This notification will contain as much information as possible as outlined in our Incident Response plan, so that affected individuals will be able to quickly and efficiently take measures to mitigate the possibility of any adverse effects.

Our incident management policies and procedures are audited as part of our SOC 2 Type II, ISO 27001, and other security assessments.

Business Continuity and Disaster Recovery

OnBoard has established Business Continuity and Disaster Recovery plans, which outline how to continue or resume services to users, and actions needed to take at the company, should critical services be disrupted.

These plans outline strategies to establish communications with employees, fully assess the disruption, actions to resume operations from backup locations, list out critical systems and backup strategies for these individual systems, and other actions that may be required.

We test and review our plans annually to ensure their effectiveness and efficiency.

Our business continuity and disaster recovery policies and procedures are audited as part of our SOC 2 Type II, ISO 27001, and other security assessments.

Log Management and System Monitoring

Internal Logs

OnBoard has implemented thorough monitoring and alerting controls in our production environment. These logs are safely stored within the Azure platform and key system logs are set for read-only access.

System Monitoring

Utilizing several tools, OnBoard performs 24/7/365 monitoring for anomalies according to our Intrusion Detection rules. If any suspicious activity is flagged, an alert is generated, and any events of interest are investigated immediately. According to our policies, we will properly manage these alerts which can involve, investigations, triage, and, if needed, the appropriate escalations.

External Validation

Security and Privacy Compliance

OnBoard is certified with SOC 2 Type II and ISO 27001, which attest to the dedication our team has to our security program and the effectiveness of the implemented controls. OnBoard also maintains compliance with applicable law and regulations, including GDPR, HIPAA, Privacy Shield, GLBA, FERPA, applicable US State Privacy Laws, and more.

OnBoard's Security and Compliance team manages our compliance program and ensures that compliance is upheld with applicable legal and regulatory obligations.

Penetration Testing

OnBoard employs a third party to perform penetration testing at least twice a year against the OnBoard application. If any findings are identified during the testing, they are reviewed appropriately and a remediation path is determined, if necessary. OnBoard makes our latest penetration testing results available within our Trust Centers Secure Resource Section.

Conclusion

OnBoard is always striving to provide the most effective and secure platform for board management, so that organizations and board members can focus on the meeting materials critical to them without nuanced distractions. At OnBoard we are always prioritizing the security and privacy of your data and are committed to continuously improving our application and practices to support this goal.

More security information is available on our Trust Center - trust.onboardmeetings.com. If you have any questions or would like to access our Trust Centers Secure Resource Section - please contact us via our Contact Page, your Sales Representative, or your Customer Success Manager.

OnBoard

BOARD INTELLIGENCE PLATFORM