Boardvantage® Security

NASDAQ BOARDVANTAGE® incorporates end-to-end security features for governance and workflow management from one central platform. Additionally, Boardvantage is hosted in an environment protected by multiple layers of security including application security, infrastructure security, process security, and physical and personnel security.

Application Security

Annual third party penetration tests are performed at least once per year.

- Medium-risk and high-risk are remediated before code updates are released to production site or mobile applications.
- An attestation letter from each third party vendor for recent penetration tests can be found in the Boardvantage Information Security Packet, which may be made available upon request where an MNDA is in place.

Involvement by Nasdaq's internal application security team for security-related matters during Boardvantage software development lifecycle.

- The Nasdaq Group Information Security Team has a role in software development lifecycle for both web and mobile applications.
    - The Information Security Team arranges for Boardvantage developers to receive secure coding training.

Encryption

- Transport Layer Security (TLS) is used by the applications to encrypt data in transit.
- All client data at rest is stored using AES-256 encryption with a unique key for each client.

Control, Auditing and Tracking

- Built–in password and user access policies
    - Unique log in per user
    - Customizable time out feature.
    - Support for 2–factor authentication.
- The application enables administrators to manage user accounts, delegate rights, adjust customizable account settings to determine access rights, and adjust other user permissions and parameters.
- The application is designed to enable administrators to generate audit reports or alert notifications showing detail such as page views, sessions, active/inactive users and password changes. This provides intelligence and visibility around user login activity, document management and alert notifications.

Mobile Device Security

- The application is designed to enable administrators to permanently render all mobile app date inaccessible in the case a device is declared lost or stolen.
- All transmissions to/from mobile applications are encrypted using Transport Layer Security (TLS) technology.
- Data is stored using AES-256 encryption with a unique keyfor each client.

Infrastructure Security

Data Centers

- Physical access to the data centers is protected 24/7, 365 days a year.
- Data centers employ documented security policies and procedures regarding access.
- Primary data centers are configured with redundant power lines, internet circuits, and UPS/generator capabilities. The US and EU and Singapore primary data centers are SSAE-16 audited.
  - High-availability
  - Multi-layered security access system
- All data centers have on-site uniformed security staff assigned to the control center for local monitoring of the AACS and CCTV activity. All data centers use:
  - Video Surveillance
  - Proximity CardReaders

Global 24/7 Security Operations Team

- The Nasdaq security operations center monitors all layers of security events related to the Boardvantage environment and its supporting infrastructure.

Antivirus

- The servers used to host the Boardvantage application have an enterprise antivirus system installed.

Network Firewalls

- Firewalls designed to provide isolation of network environments and network access control protection.

APPLICATION SECURITY

INFRASTRUCTURE SECURITY

PHYSICAL & PERSONNEL SECURITY

PROCESS SECURITY

Host Intrusion Detection Systems (HIDS)

- HIDS technology is deployed throughout the Boardvantage server infrastructure.

Intrusion Detection Systems (IDS)

- Intrusion Detection Systems/Intrusion Prevention Systems – IDS/IPS technology are deployed throughout the application infrastructure.

Network Segmentation

- VLAN and physical segmentation.

Network Access Controls

- Controls are in place for corporate internally managed networks.
- Nasdaq has strict controls around production network access, including 2-factor authentication.

Web Application Firewalls (WAF)

- WAFs are deployed in blocking mode protecting Directors Desk.

Personnel Security

Code of Ethics

- Company policy is that each employee must annually certify understanding of and compliance with Nasdaq Code of Ethics.

Security Awareness Training

- Yearly Security Awareness Training is required by policy for all employees, as well as regular training sessions for software and hardware engineers regarding industry security best practices.

Process Security

Dedicated Information Security Team

- The Nasdaq Group has a dedicated Information SecurityDepartment headed by the Chief Information Security Officer who reports to the Chief Information Officer.

Internal Application Security Team

- The staff within the Nasdaq Information Security Department is regularly provided training in advanced information security concepts.
- Additional oversight of the Boardvantage application is provided by The Nasdaq Group's Internal Audit Department

Disaster Recovery and Business Continuity

- In the event of a system or data center failure, client application requests will be redirected to the disaster recovery site if required. To facilitate timely failover between facilities, disaster recovery plans have been created and are tested on a yearly basis. Boardvantage is designed for failover recovery times (RTO) of less than four hours and recovery point objectives (RPO) of less than 8 hours.
- Nasdaq has developed a comprehensive internal Business Continuity Plan that facilitates the continuation of client services and system support in the event of issues affecting standard operations, such as a force majeure event. The plan is kept current and tested on a periodic basis.

Backups

- The Boardvantage service is designed to perform regular backups of client and system data to ensure continuity of service in the event of a primary data center or system failure. Client content is replicated in near-real time between primary and secondary data centers and backed up to a server based archival system on a nightly basis.

Soc 2 and ISO 27001

- Boardvantage Inc.[1] is SOC 2 certified and the Information Security Management System (ISMS) that governs the information assets, business operations and physical locations for the Board Portal Services/ Boardvantage conforms to ISO 27001 requirements and is ISO 27001 Certified.

Risk Assessment Discipline

- Group Risk Management (GRM) is ultimately responsible for governing, developing, coordinating and controlling the Enterprise Risk Management process and providing relevant support to the line organization.
- GRM is responsible for the Nasdaq-wide risk reporting process and the aggregation of detailed risk information to a consolidated risk portfolio.
- GRM also provide consistent and continuous information on risk exposures and current risk trends to Executive Management and the Board of Directors.

[1] Boardvantage Inc. is a wholly-owned subsidiary of Nasdaq Corporate Solutions, LLC, which itself is a wholly-owned subsidiary of Nasdaq, Inc. The information provided in this document applies to the standard MeetX SaaS Solution hosted by Nasdaq and its Affiliates, and does not apply to MeetX's On Premise or Private Cloud offering.

Boardvantage is a service provided by the Corporate Solutions business of Nasdaq, Inc. This brochure is provided for information only. For terms and conditions applicable to use of the Boardvantage service, prospective customers please refer to Corporate Solutions' master services agreement, and current customers please refer to your contract with BoardVantage, Inc. for MeetX.

0420-Q17