MINDPRO

OUR SECURITY MEASURES

MINDPRO – SECURITY MEASURES

_SECURITY & ORGANIZATIONAL STRUCTURE

Mindpro, who provides the portfolio of cloud apps in the Atlassian Marketplace, is a brand name for the innovation and software development department at e-Core IT Solutions ("Company", "we", "us", or "our").

Given this legal structure, Mindpro abides by e-Core LLC Information Security policies, which can be requested on demand at: security@mindproapps.com or by raising a security request here. In addition to this, as part of our company structure, we have a dedicated InfoSec team composed by three security specialists with the specific roles described below. This dedicated team is organized to work with Mindpro's developer and support team in case of any privacy, security, or compliance need:

- Governance Specialist: The focal point for laws and regulations related to information security.
- Cybersecurity Specialist: The focal point for information security tools, including device management, antivirus, alert systems, vulnerability identification systems, and password vaults.
- Senior Security Analyst: Focal point for numerous security activities, from reviewing policies and participating in audits to managing our tools to protect the company.

_TECHNOLOGICAL & ORGANIZATIONAL MEASURES

Learn about the measures we take to improve our technological and organizational company security. All measures listed below have been implemented and are followed by all our employees:

- All mobile IT assets must have encrypted hard drives.
- All employees have an exclusive username and password with at least 12 characters.
- All IT assets must be network isolated by VLAN segregated by team or business line.
- All computers are screen saver locked after 5 minutes idle.
- All computers and servers must have antivirus/endpoint protection active, weekly scanned, and daily updated.
- All computer/access data will be wiped out after a user termination.
- All accesses to IT assets, computers, applications, and software are based on the least privilege required for the business.
- All devices accessing corporate resources or critical systems must have a Mobile Management agent installed.
- All networks, firewalls, gateways, routers, and assets are monitored by the network and host intrusion detection system.
- All assets must have up-to-date operational systems.

- All systems, applications, firewalls, entrance, web surfing, and behavior may be monitored and investigated without prior notice.
- All employees should attend annual and recurrent Information Security, Cyber Security, and ethical awareness training, understanding and accepting our terms and remaining vigilant to threats and attacks.
- All assets (servers, workstations, network devices, web applications, etc) are subject to vulnerability assessments and penetration tests.
- All employees' assets are subject to recurrent internal audits conducted by the Information Security team.
- Multi-Factor authentication is enabled to access corporate critical, confidential, and collaborative systems.
- All operational systems patches and updates are applied automatically using our Mobile Device Management resource.

_SECURITY MANAGEMENT

Learn more about our secure development, change, release, and incident management practices.

Secure Development - These are some of the secure development practices we apply in our activities:

- We groom developers security champions with dedicated time to learn and implement security practices in your app and we have periodic technical security training for the whole team.
- We have enforced multi-factor authentication in all our source code repositories.
- We do regular peer-reviews of code and infrastructure within our development team to ensure high code quality and security awareness.
- For every change in code, GitHub actions are run, which build the app and scan for vulnerabilities in code using Snyk, Sonar and npm audit tools. If any critical or high vulnerability is found, the build is set a "failed" and is not merged into the main branch. Then it is corrected until it passes.
- In addition to these practices, we self-check other security rules from top security standards such OWASP Top 10 (Open Web Application Security Project) to strengthen our reviews.

Incident Management - The steps below represent a high-level overview of our app's security incident management procedures:

- We are constantly monitoring our environment and infrastructure, and we always have at least one Engineer "on call" in case of need.
- If an issue is identified and classified as a security breach, we'll immediately set up an incident response team responsible for handling the situation.
- We'll assess the security breach and vulnerability level according to CVSS v3.
- We'll determine the root cause, for how long the issue might have been present, and which users were affected (if any).
- We'll notify and create a Security Incident Ticket with Atlassian Support (no later than 24 hours).
- We'll work with all team members required (from Engineering, Security, and Support) to resolve the issue following the remediation dates and SLAs defined in the Atlassian Security Bugfix Policy.
- Depending on the context and impact on the potentially affected customers, we'll send these customers a notification email informing them about the security breach, the action plan, and the respective SLAs to resolve the issue.
- We'll resolve, test, and publish the security fix.
- We'll take corrective actions to prevent similar incidents from happening in the future.
- We'll notify Atlassian Support, close the ticket, and inform the affected customers.

_SECURITY PROGRAMS

All Mindpro apps adhere to all of the security requirements and programs enforced by Atlassian for all

Marketplace Vendors and Apps:

App Security Requirements - Cloud App Security Requirements are a set of mandatory requirements Atlassian defined for all Marketplace Partners. Atlassian audits Marketplace Partners against these requirements yearly to ensure they adhere at all times. Mindpro fulfills these security requirements and passes the audit successfully every year.

Ecoscanner - Ecoscanner is Atlassian's platform to perform security checks against all Atlassian Marketplace cloud apps on an ongoing basis. Mindpro cloud apps are continuously monitored by Ecoscanner. This process brings possible vulnerabilities to light very early so we can address them before they cause any damage.

Vulnerability Disclosure - The Vulnerability Disclosure Program is a reporting platform run by Atlassian, providing a safe and effective way for Atlassian, customers and security researchers to report vulnerabilities. Mindpro cloud apps are participating in this program.

Security Bug Fix Policy - The Security Bug Fix Policy defines specific Security Bug Fix SLAs that all Marketplace Partners are expected to meet. This is to ensure cloud app vulnerabilities are addressed promptly and eventually fixed. Mindpro adheres to these SLAs.

_DATA MANAGEMENT

Data Storage & Protection - Each product needs to access and store a specific data group. In addition, the way this group of data is stored and managed also varies according to the Atlassian Development platform the app was developed on, if on the 1) Atlassian Connect platform or 2) Atlassian Forge platform.

Mindpro Apps built on Atlassian Connect - We have two products running on this platform, they are: Mindpro Sync and Mindpro Deliver:

- Our apps running on the Atlassian's Connect platform have their data stored and managed using Mindpro's own cloud infrastructure that runs on top of AWS data centers.
- Our Amazon AWS's RDS database is located at US-West Virginia and the legal region is Brazil.
- All data is encrypted at rest using military-grade AES-256 encryption. High risk data have multiple levels of encryption applied.
- Amazon AWS's data center are SOC-2 compliant and providing a wide range of industry-specific compliance certifications. These certifications address a range of security controls including physical and environmental security and protection. See here for more details: Amazon Aws Cloud Compliance
- The Mindpro team accesses application data only for purposes of application health monitoring and performing system or application maintenance, and upon customer request for support purposes.
- Access to customer data requires authentication and authorization controls, including Multi-Factor Authentication (MFA).
- All employee access to systems is logged and audited for security purposes and as part of their contract of employment all Mindpro employees have to sign Confidentiality Agreements and Non-Disclosure Agreements.

Mindpro Apps built on Atlassian Forge - We have four apps running on this platform: Mindpro Insights, Mindpro Lineup, Mindpro Graphy and Mindpro Dashio:

- Our apps built on Forge run directly on an Atlassian-hosted cloud platform.
- Due to the nature of this hosting on the Atlassian infrastructure, all customer data is stored and managed directly in Atlassian's Forge Storage environment.
- That is, the stored data of this app built on Forge is not hosted in any Mindpro infrastructure / database.

Backup & Recovery - We have structured a series of measures and practices to guarantee your data's backup and recovery in extreme events:

- We are fully hosted on AWS, which is 100% fault tolerant. Thus, we automatically benefit from the expertise and high availability provided.
- Additionally, we have redundancies built in to keep the application running in the event of an outage in the region.
- We make snapshots of the AWS RDS databases every 24 hours to provide backup and redundancy in case of failure, and we can restore up to 7 days of customer data from these stored backups.
- Our Recovery Time Objective (RTO) is 1h and Recovery Point Objective is 24h.
- Recovery scripts are in place, and they can be replicated in another AWS region if our primary region has a severe outage.

_APPS SECURITY STATEMENT

As each product accesses and stores different data, we provide each with its own Data & Security Statement. Click on the links below to read the statement for the product you're interested in:

- Mindpro Sync - Security & Privacy
- Mindpro Insights - Security & Privacy
- Mindpro Lineup - Security & Privacy
- Mindpro Graphy - Security & Privacy
- Mindpro Dashio - Security & Privacy
- Mindpro Deliver - Security & Privacy