Encryption

Last Updated: 15 January 2025. **Author:** Max Lindsay. This document gives a comprehensive breakdown of our encryption and how it is utilized to keep your data safe:

AES-256-bit Security Encryption:

BoardCloud uses AES-256 bit security specification to encrypt all documents stored on our servers. This includes uploaded documents, documents originating on the platform as well as ancillary documents such as cover pages and packet divider pages.

Document Sharing:

Uploaded documents are encrypted as they are transferred after which the source documents are deleted. From then on, requests to open, view or edit any document are authenticated based on the Group and Role permissions of the requesting user, before being unencrypted for reading purposes.

Our document links are hashed, meaning that if someone shares or emails a BoardCloud document link, the user opening the link will have to authenticate themselves before accessing the content.

Encryption Management System:

Data at rest is encrypted using Advanced Encryption Standard (AES) with a 256-bit key length, a globally recognized and highly secure cryptographic algorithm. This standard is used to secure documents, files, and any other stored data within our platform, preventing unauthorized access even in the event of a physical security breach. Encryption keys are managed securely, employing a hierarchical key management system that includes regular key rotation and strict access controls to minimize risk.

Secure Data In Transit:

For data in transit, we utilize Transport Layer Security (TLS) protocols to provide robust encryption during communication between users and our servers. This ensures that any information exchanged, whether login credentials, sensitive documents, or administrative settings, is protected from interception and tampering. Our TLS configuration adheres to industry best practices, including support for only strong cipher suites and protocols, such as TLS 1.2 and TLS 1.3.

End-To-End Encryption:

In addition to securing stored and transmitted data, BoardCloud offers end-to-end encryption for specific use cases. This ensures that sensitive information remains encrypted from the moment it leaves a user's device until it reaches the intended recipient, with no opportunity for decryption along the way. Such measures guarantee that even in a scenario where our servers are compromised, the data remains secure and inaccessible to unauthorized parties.

This document is intended for prospective and current customers seeking an overview of BoardCloud's security measures. For detailed technical documentation, please reach out to our support team.

Regulatory Standards:

To further enhance security, all encryption operations are conducted in compliance with global standards and regulatory requirements. BoardCloud's encryption practices align with the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other relevant frameworks. This ensures that our clients' data is protected not only technically but also in accordance with legal obligations.

Key management is an essential part of our encryption strategy. Keys are stored in a secure Key Management System (KMS) that utilizes hardware security modules (HSMs) for enhanced protection. This approach prevents unauthorized access and ensures that keys are only accessible to authenticated systems and personnel. Moreover, periodic audits and reviews of our encryption policies and practices are conducted to maintain their efficacy and address emerging threats.

Backup Encryption:

Uploaded documents are encrypted as they are transferred after which the source documents are deleted. From then on, requests to open, view or edit any document are authenticated based on the Group and Role permissions of the requesting user, before being unencrypted for reading purposes.

Future Developments:

BoardCloud continually monitors advancements in cryptographic technologies to ensure our encryption practices remain state-of-the-art. By employing cutting-edge algorithms, secure key management practices, and robust implementation strategies, we provide a secure environment for our clients to manage their board activities confidently. Encryption is not just a feature of our platform; it is a commitment to the highest standards of data protection and trust.

Contact Us:

For more information about BoardCloud's security features, please contact us at info@boardcloud.org or visit our website at www.boardcloud.us.

This document is intended for prospective and current customers seeking an overview of BoardCloud's security measures. For detailed technical documentation, please reach out to our support team.