HOIST

DATA SECURITY AND PROCESSING

HOIST is dedicated to ensuring the security and confidentiality of data entrusted to us by our customers. As a Software as a Service (SaaS) provider, we recognize the critical importance of maintaining robust data security standards and procedures. This document outlines the data security standards and procedures that govern the handling, storage, and protection of data within the HOIST SaaS software platform.

Data Classification

- All data within the HOIST platform shall be classified based on its sensitivity level (e.g., public, internal, confidential, highly confidential).
- Data classification shall dictate the appropriate security controls and access permissions applied to the data.

Access Control

Access to the HOIST platform shall be role-based, with permissions granted based on the principle of least privilege.

- Users shall authenticate using strong, multi-factor authentication mechanisms.
- Access to sensitive data shall be restricted to authorized personnel only.
- Access logs shall be maintained and regularly reviewed for any unauthorized access attempts.

Encryption

- Data transmission over networks shall be encrypted using industry-standard encryption protocols such as TLS.
- Data at rest shall be encrypted using strong encryption algorithms.
- Encryption keys shall be securely managed and rotated periodically.

Data Handling

- Data shall be processed, stored, and transmitted securely in accordance with applicable laws and regulations (e.g., GDPR, CCPA).
- Data shall only be accessed and processed for legitimate business purposes.
- Data masking techniques shall be employed where appropriate to protect sensitive information.

Vulnerability Management

- Regular vulnerability assessments and penetration testing shall be conducted to identify and remediate security weaknesses.
- Security patches and updates shall be applied promptly to mitigate known vulnerabilities.

Incident Response

- An incident response plan shall be in place to effectively respond to and mitigate data security incidents.
- All security incidents shall be promptly reported, investigated, and documented.
- Remediation actions shall be taken to prevent recurrence of security incidents.

Data Backup and Recovery

- Regular data backups shall be performed to ensure data integrity and availability.
- Backup data shall be stored securely and tested periodically for recoverability.
- Procedures for data restoration in the event of data loss or corruption shall be documented and tested.

Physical Security

- Physical access to data centers and server rooms hosting the HOIST infrastructure shall be restricted to authorized personnel only.
- Environmental controls such as fire detection and suppression systems shall be implemented to safeguard physical infrastructure.

Employee Training and Awareness

- All employees shall receive training on data security policies, procedures, and best practices.
- Regular security awareness programs shall be conducted to promote a culture of security consciousness among employees.

Compliance and Audit

- Compliance with data protection laws, regulations, and industry standards shall be regularly assessed.
- Independent third-party audits shall be conducted periodically to evaluate adherence to security standards and procedures.

Conclusion

HOIST is committed to maintaining the highest standards of data security to protect the confidentiality, integrity, and availability of data within our SaaS software platform. By implementing the above standards and procedures, we aim to provide our clients with the assurance that their data is handled and protected with the utmost care and diligence.