The Honest Company, Inc. Data Transfer Security Requirements

Effective as of October 26,2022

Introduction

The Honest Company transfers data (within the Honest private network and over the Internet) for a number of business functions supporting eCommerce and internal company operations.

Encrypting data in transit can be an effective control to protect company data from unauthorized access and breach disclosure under safe harbor rules.

Definitions

Cleartext data that is not encrypted

Ciphertext data that is encrypted

Protocol technology standard for data exchange

NIST - National Institute of Standards and Technology

Transport Layer Security (TLS) - standard protocol for transferring encrypted data **Regulated** - data that is subject to contractual obligations, state, or federal law

Policy Requirements

Data and Information Protection Management

- All information and information systems must be safeguarded to prevent unauthorized access or modification, misuse, loss, damage, or theft.
- Employees and non-employees with access to non-public information are responsible for protecting Company information from unauthorized access, modification, duplication, destruction, or disclosure whether accidental or intentional. Software, Systems and Service Assurance
- A technology acceptable use policy must be documented and published to employees

Information Ownership and Handling

- Confidential data may be collected or retained for legitimate business purposes only. Refer to the Backup, Retention, and Recovery policy for more details.
- Backup data or media must be stored at a secured off-site location.
- Only the minimum amount of confidential information required to conduct business may be collected and retained.
- Business Units must determine whether a legitimate business purpose exists for collection and retention of confidential information.

Information Asset Management

- All information systems must be identified and information about the information system must be maintained in a Company approved asset management/ inventory system.

- This information includes, but is not limited to asset name, asset type, product name, software/hardware vendor, version numbers, current state of deployment, location, and the name of the person or role within the Company responsible for the asset.

Information Disposal

- A critical part of safeguarding sensitive information is properly disposing of it when information is no longer needed, its retention period has expired, and information is not required to be retained as directed by the Legal Department and/or pursuant to a Legal Hold.
- Unauthorized destruction or disposal of THC's records or information by an individual may subject the individual to disciplinary action up to and including termination and possible prosecution.
- Information must be disposed of according to the most current publication of NIST SP 800-88 "Guidelines for Media Sanitization." In the event a third-party vendor is used to dispose of media, certificates of destruction or sanitation must be provided by the vendor.

Suspected Data Loss or Unauthorized Disclosure

Disclosure of Company information to an unauthorized party, or the suspected loss or disclosure to an unauthorized party, must be reported promptly to the IT Support or Information Security. Refer to the Cybersecurity Incident Response Plan (CSIRP) for more detailed guidelines, processes, and responsibilities.