The Honest Company, Inc. Information Security Policy

Data Transfer Security Requirements

Effective as of November 1st 2015

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

- In order to protect the confidentiality and integrity of the company's sensitive data, any Regulated or confidential data **SHALL** be transmitted via encrypted communication to ensure that it does not traverse the network in cleartext.
- All data that is Regulated or confidential **SHALL** be transferred using NIST-approved encryption standards and protocols.

Responsibilities

All Business Units - Ensure internal & 3rd party applications that are used meet or exceed this policy. If requirements cannot be met, business unit must obtain a documented security policy exception (approved by the CTO and CFO).

Information Security Department - Develop and maintain data transmission policy and associated standards

Appendix A - Examples of Secure Data Transfer

This list is representative of common applications and encryption used, but is not complete.

Web-Based Applications
Encryption of confidential or regulated data between a user's browser and a web-based application MUST be over secure protocol (such as TLS)

File Transfers
Encryption of regulated or confidential files can be via Secure Copy (scp), Secure FTP (sftp), approved 3rd party software (i.e., Dropbox, Google Drive)

E-mail
Confidential data transmitted in e-mail MUST be encrypted prior to being sent (i.e., can be shared using approved 3rd party tools such as Dropbox and Google Drive).

Interactive Sessions
When accessing systems remotely use secure access (i.e., SSH).