

The Honest Company, Inc.

Information Security Policy

Laptop & Desktop Data Encryption Policy

Effective as of October 15th 2016

Introduction

The purpose of the Laptop & Desktop Data Encryption Policy (this “Policy”) is to ensure that all information of any kind that is stored on laptop and desktop computers which have been issued to employees of The Honest Company, Inc. (“Honest”) shall have Full Disk Encryption[1].

Data encryption protects data from unauthorized access and reduces and/or eliminates breach reporting requirements in case of lost or stolen devices.

*If an Honest employee loses sensitive data on a laptop and/or desktop computer that **is not encrypted in accordance with the terms of this Policy, such employee may be subject to disciplinary action, up to and including termination.***

This Policy pertains to data-at-rest encryption requirements (i.e., data residing on an employee laptop or desktop computer(s)). For data in transit requirements, see published policy “*Information Security Policy - Data Transfer Security Requirements*”

Definitions

Encryption - The process of transforming information to make it unreadable to anyone except those possessing a key.

Laptop computer – A portable, usually battery-operated Personal Computer, small enough to rest on a user’s lap.

Desktop computer - A personal computer designed for regular use at a single location on or near a desk or table.

Scope

This Policy applies to all laptop and desktop computers owned by Honest. Data encryption or other similar requirements for other mobile devices (i.e., smartphones, tablets, etc.) will be governed by subsequent policy releases.

*Note: This Policy **does not** apply to server infrastructure.*

Responsibility

Employees and Contractors

It is the responsibility of Honest employees to understand and comply with this Policy and any corresponding procedures.

Information Technology

Implement this Policy according to standards set in Appendix A.

Information Security

Enforce and update this Policy, including approved solutions in Appendix A.

Policy

- 1. All laptop and desktop computers issued by Honest and/or used by Honest employees must be equipped with Full-Disk Encryption.**
- 2. Only encryption products approved by Information Security (See *Appendix A*) and configured by Honest according to standards set by Information Security may be used to encrypt computers under this Policy. It is a violation of this Policy for users to use any other products and/or tools to encrypt any laptop or desktop computer governed hereunder.**

3. It is a violation of this Policy for anyone to bypass, penetrate, alter the configuration of, or to otherwise modify or attempt to modify in any way the operation of any encrypted laptop or desktop hard drive(s).

4. If an employee loses sensitive information on a laptop or desktop computer that is not encrypted in accordance with the terms of this Policy, such employee may be subject to disciplinary action, up to and including termination of employment.

Appendix A - Authorized Encryption Products

- Native OS Encryption Products
 - Apple FileVault
 - Microsoft BitLocker
- 3rd Party Encryption Product
 - McAfee EndPoint Encryption
- 3rd Party Key Management
 - McAfee ePO
 - JAMF

For any questions regarding this policy, requests for exception or modification contact security@honest.com

[1] Full Disk Encryption is encryption of the entire contents of a hard drive(s), not file or folder level encryption.