The Honest Company, Laptop & Desktop Data Encryption Policy

Effective as of October 26, 2022

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.

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.

Policy

Password Policy and User Authentication

- Strong encryption cryptography must be used for transmission of authentication credentials
- User authentication requires at least something you know (e.g., password) or something you have (e.g., token) or something you are (e.g.,
- biometric).
- User accounts must be locked out after 6 failed login attempts.
- User account lockout duration must be set to a minimum of 60 minutes or until an administrator unlocks the account.
- Passwords or passphrases must be complex in nature requiring a minimum length of 10 characters that meet 3 out of 4 following criteria:
- Uppercase letter (A-Z)
- Lowercase letter (a-z)
- Numeric character (0-9)
- Special character (i.e., !, $, #, or %)
- Passwords or passphrases must be changed at least once every year. Passwords for cloud-based applications may expire more frequently
- depending on the technical limitations of the system.
- The last four passwords or passphrases must not be re-used.

Wireless Network Devices

All wireless network devices are required to support and use strong encryption technologies (i.e., WPA2) for both authentication to the network and transmission of data. A mechanism must be in place to detect unauthorized wireless networks or devices and be able to distinguish between various types of wireless devices.

System Access, Passwords and Security Parameters

Only authorized and approved devices, including USB or other external storage devices, may be used to access, store or process non-public information. Limited exceptions may be granted with proper business justification provided and approval from the employee's manager and HR business partner. All network connections must be logged, centrally managed, properly secured, approved, and periodically audited. Remote access must be limited to authorized users and only allowed through the Company approved mechanisms. All vendor-supplied defaults must be changed on all system components before installing the device on the network. (e.g., passwords, simple network management protocol (SNMP) community strings, etc.). All unnecessary default accounts must be removed or disabled before installing the device onto the network. The encryption keys, passwords or passphrases must be changed anytime anyone with knowledge of the credentials leaves the company or moves to a position that no longer requires knowledge of the credentials. All encryption keys utilized must be securely distributed and stored. Strong cryptography (i.e., SSH, VPN, TLS 1.3) must be used for any non-console or web-based management interface used for administration of systems or system components. Separation of duties must be in place between personnel working in the development/test environment and those working in production environments.