The Honest Company, Inc. Information Security Policy

User & Service Provider Security Standards

Effective as of July 16th 2015

Introduction

Employees, contractors and guests ("Users") of The Honest Company, Inc. ("Honest") may from time to time be assigned an electronic account by the Information Technology department and/or other groups within Honest.

A User username and password, also referred to as a credential, identify the User for access to any number of internal or external electronic accounts (such as CRM, training platform, financial system, etc.).

The purpose of this Security Policy is to establish security standards to protect the confidentiality, integrity, and availability of Honest's electronic accounts and assign responsibility to both Users and Service Providers (as defined below) for the proper use and safeguarding of credentials.

Definitions

Authentication is the process by which a User proves his or her identity (at a minimum with a username and password; see Two Factor Security below) to gain access to a particular electronic account.

Identity Provider is a trusted provider that enables a User to use single sign-on to access other websites and applications.

Service Provider provides computing resources to Honest Users electronically (such as CRM, training platform, financial system, etc.).

Two Factor Security or Multi-Factor Security is a stronger form of Authentication where a username and password is combined with another factor (such as a phone or token) for enhanced authentication related to particular electronic account.

Service Account is an account that belongs to an application instead of to an individual end user.

Policy Requirements

Users

Users may be given access to a Honest account, at which time a User should establish a username and password for purposes of authenticating the account. It is the responsibility of the User to safeguard their credentials to prevent any unauthorized access to all Honest accounts and the services or resources accessed thereby.

Users MUST NOT share or disclose their account credentials. If Users require machine-to-machine or application-to-application connectivity, a different account, referred to as a Service Account (*see definition above*), MUST be requested.

Users are required to promptly notify Honest's Information Security department if they become aware that their account has been accessed by another party. Immediately thereafter, depending on the severity of the account compromise, Information Security will either require the User to change his or her account credentials or deactivate the account.

Honest may suspend or revoke User access to systems that do not meet security standards.

Service Providers

Service Providers SHALL be required to comply with Honest standards (see below) for Identity & Access Management (IAM). Service Providers that do not comply to these standards must have an exception approved by Honest's CTO & CFO.

Service Provider Standards

- Authentication MUST be encrypted and session must continue to have encryption (i.e., a session may not start with HTTPS and downgrade to HTTP)
- Authentication MUST NOT be saved (i.e., usernames and passwords)
- Authentication MAY require Two Factor Security, depending on the resource accessed
- Allowable Identity & Access Platforms Services
    - Active Directory, Honest instance
    - RADIUS, using Honest Active Directory as source for RADIUS Server identity
    - SAML, using authorized Identity Provider (*See Appendix A*)
    - OAuth, using authorized Identity Provider (*See Appendix A*)

Appendix A - Authorized Identity Providers

- Authorized Identity Providers for Honest:
    - Google Apps - The Honest Company account
    - Microsoft Azure - The Honest Company account
- Additional Identity Providers can be sent to Information Security for evaluation.

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