The Honest Company, Inc. User & Service Provider Security Standards

Effective as of October 26, 2022

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

Identity, Access, and Entitlement Management

- Access to non-public information must be limited to employees and non-employees with appropriate authorization.
- Access to information systems must be limited to uniquely identified users or system resources with appropriate authorization.
- Authorization must conform to the principles of least privilege (most restrictive) and need-to-know basis and only for the minimum amount of time necessary.
- Account creation must follow a documented process that includes procedures for approving access by the employee's manager and information owner.
- Account creation and the process of account authorization must be auditable.
- Accounts must be used only for their approved and intended purpose and for no other reason.
- A formal process must be in place for granting, revoking, or transferring user access to all Company information and information system.
- To help ensure authorization and appropriateness of access rights, all accounts with system access (including end-user, privileged/administrator, generic, and system/service accounts with access to the application, operating system, and database) must be reviewed at least annually, or more frequently based upon the needs established by the business and/or IT management.
- Following the User Access Review process, access review must be performed by IT and/or business personnel who have knowledge and authority to determine whether a user and his/her access within the system is appropriate based on job functions, and if the access constitutes a segregation of duties conflict. The determination should adhere to the principle of least-privilege: users should only be assigned access that is essential for them to perform their job functions. Any access change requests, as a result of review, are to be processed timely.

Third-Party Access

- Access for non-employees to Company information systems and/or non-public information must not be provided until a contract has been signed defining the terms and conditions for the use of THC information systems and/or non-public information.
- Contracts with non-employees who obtain access to THC non-public information or information systems and contracts with such individuals' employers must require compliance with relevant information security requirements.
- Access for non-employees must only be activated or extended after supervisor and legal or HR approval, assigned a termination date in the access control system, and must not exceed one year.
- Only activate remote-access technologies for vendors and business partners when needed and immediately deactivate remote-access sessions after use.
- IT will verify with the respective department, functional team, or manager the status of the contractor account once every month. If no response is provided within seven days of notification, the contractor account will be disabled and the manager must submit a ticket to the IT Help Desk to reactive the account.

User Accounts

- All systems containing non-public information are required to utilize at least an account ID and password/PIN combination authentication mechanism.
- Unique IDs must be used for all user-level access.
- The use of shared and generic accounts are restricted to systems where the use of individual accounts are technically not feasible or costprohibitive.
- All shared accounts must be properly documented by the requesting department and approved by the Director, IT Infrastructure and Operations.
- Access to all systems must be disabled within 24 hours of user termination date or requested access removal date.
- Inactive user accounts must be deactivated if not in use longer than 90 days.
- Company-owned computer and assets must be returned upon termination.
- Deactivated accounts covered under User Account Review.
- Administrators must verify the user identity before modifying credentials.