IT Security Policy

Version Control History

Version	Date	Description	Author	Approved By
1.3	09/2020	Updated contact information, vendors, and process	Thomas Yang	
1.4	08/2021	Added Offboard, onboard, introduction, scope, 1.6.4 Privileged Access, 8.0 Audit Controls and Management, 1.3.5 added deactivated accounts covered in UAR	Doug Nguyen, Thomas Yang	
1.4	12/8/2021	Reviewed and Approved		Sherry Parvaneh
1.5	1/20/2022	Updated section 5.5.5 to specifically restrict access to USB and other external storage devices	Doug Nguyen	
1.6	10/26/2022	Updated Roles and Responsibilities, removed undocumented exceptions, moved version control history to the front, employee handbook reference	Rokas Venckus	Brendan Sheehey

1.0 Overview

The primary mission of IT Security is to protect The Honest Company ("Company") brand, technology, and digital assets by minimizing the company's risk and exposure to external and internal threats. Unauthorized access or disclosure, modification or deletion of company information can compromise business operations and individual privacy rights. As a result, it is our collective responsibility to ensure we maintain:

- Confidentiality of all non-public information from unauthorized access
- Integrity and Availability of all information stored on or processed by Honest systems
- Compliance with applicable regulations, laws and company policies

Violations of these policies, knowledge of vulnerabilities and all other security incidents must be reported to Information Technology Department.

2.0 Purpose

This policy establishes a framework to protect information critical to The Honest Company's operations and as required by contractual agreements and applicable laws. This policy defines standards and minimum requirements for managing security to ensure Company data and digital resources are appropriately protected from accidental, unauthorized, or malicious modification, destruction, and disclosure, and these protections are accomplished in a manner consistent with the company's requirements.

3.0 Scope and Policy Statement

3.1 Scope

The IT Security policy applies to all computer devices, applications, databases, and other components ("systems") and to all parties operating within the Company's network environment or utilizing Company systems, including board members, directors, employees, contractors, consultants, business partners, and any third-party users. Upon hire and annually thereafter, employees are required to attend Cybersecurity Awareness training and agree to abide by the applicable standards and procedures outlined in this policy.

This policy applies to processes related to IT Security management for systems and the related supporting infrastructure that are owned, licensed, or otherwise possessed by the Company, including certain software as a service (SaaS) applications.

For systems where it's technically not feasible or financially cost-prohibitive to comply with one or more requirements defined in this policy, compensating controls must be implemented to mitigate the risks associated with these exceptions. All exceptions must be documented and approved by the Chief Information Officer and the Director, IT Infrastructure and Operations.

3.1.1 Exceptions

Application Name	Policy Exception(s)	Approval

3.2 Policy Statement

Policies are general guiding principles and objectives for the business. Standards are specific rules or uniform methods that support a policy.

Policies and standards will be reviewed and if necessary augmented annually. This process will certify our protection measures remain purposeful and relevant.

This policy document will also be reviewed at least annually by the custodian(s) (and any relevant data owners) and updated as needed to reflect changes to business objectives or the risk environment.

The IT Security policy operates in conjunction with applicable laws, regulations and Employee Handbook. Laws and approved exceptions may supersede the outlined policies or standards.

As a company, we are required to comply with many state, federal, international and industry regulations. Below are two important mandates we must adhere to:

Notification of Security Breaches (California Civil Code 1798.80-1798.84). Requires reasonable steps for destruction of personal information no longer to be retained; requires notification of California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person due to a breach of security of a computer system.

Payment Card Industry Data Security Standard (PCI DSS v3.2) In order to properly protect card holder data (CHD), PCI DSS requires (overview):

1. Build and maintain a secure network and systems
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

4.0 Roles and Responsibilities

4.1 Chief Digital And Strategy Officer, Chief Information Officer/VP of Technology

Responsible for oversight and supports the IT Security policy. Reviews and approves policies and ensures alignment at the senior leadership level. Has overall accountability to meeting the IT Security policy mandates.

4.2 General Counsel

Responsible for ensuring the information security and information technology programs are aligned with legally mandated and regulatory requirements. Legal will also review and identify legislation that impacts security policies.

4.3 Director, IT Infrastructure and Operations

The Director, IT Infrastructure and Operations is the owner and responsible for the development and maintenance of the IT Security policy. Policies are reviewed and approved by the CIO/VP of Technology, General Counsel. Standards are approved by the Director, IT Infrastructure and Operations. Additional responsibilities may include:

- Owns, establishes, and manages strategic direction for the security program
- Drives Governance, Risk and Compliance to the security program
- Develops and oversees security awareness program
- Ensures Business Unit and Technology alignment to the security program

4.4 Cybersecurity Engineer

The Cybersecurity Engineer is responsible for designing and implementing information security systems and solutions that adhere to technical standards and security policies and aim to better secure Company information and systems. Additional responsibilities:

- Maintains information security protection policies and standards by ensuring their alignment with adopted security frameworks and best practices
- Aligns security and technology architecture
- Develops and maintains secure configuration standards
- Consults and reviews new and existing business systems and applications for compatibility to security architecture and adherence to protection policies and standards

4.5 Security Operations

Security Operations is responsible for protecting the Company’s technology and digital assets by monitoring, preventing, detecting, investigating, and responding to cybersecurity threats.

4.6 Human Resources

Human Resources is responsible for ensuring the employee handbook references and is aligned with information protection policies. As part of their regular duties, HR will conduct background checks to ensure the workforce is properly vetted before they are permitted to access information assets belong to the Honest Company.

4.7 Management

Management is responsible to manage risks to information and information systems by ensuring information protection policies are understood and implemented in their respective areas of duty. Additional responsibilities:

- Ensure their staff understand and implement information protection policies
- Ensure their staff complete required security awareness training
- Ensure their staff return company-owned equipment upon separation from the company
- Manage and review staff access and entitlements to information and information systems to ensure the policies of separation of duties, least privilege and need-to- know are followed.
- Develop and maintain business continuity plans for critical business functions and services

4.8 Privileged Users

Privileged users are individuals who are responsible for implementing, supporting and developing technology (e.g. networking, applications, hardware, web services and programs, databases and workstations) as well as those who have permissions to view, modify and delete Company information classified as Restricted. Additional responsibilities:

- Understand the Information IT Security policy requirements for their area of responsibility
- Ensure their technology is securely deployed with the appropriate security controls and in conformance with the IT Security policy
- Maintain an inventory of assets under their control
- Diagram all systems documenting internal and external connections
- Document supporting guidelines for information assets and systems under their control
- Consult with Information Security when implementing a new technology or in support of existing technology services to ensure alignment with the IT Security policy
- Privileged users that handle Restricted data must ensure information is stored in a secure place and accessed only according to security controls

4.9 Data Owner

Data or Information Owners are authorized personnel in each respective business area assigned to oversee the creation, use, and access to business information. Additional responsibilities include:

- In partnership with the Data Custodian (technology personnel), ensure data is maintained at the appropriate confidentiality, integrity, and availability level.
- Ensure access to data is based on job role and is alignment with the policies of least privilege and need-to-know.

4.10 Data Custodian

Data or Information Custodian are authorized support personnel in each respective technology area assigned to protect business information and /or the system handling and storing the information. Additional responsibilities include:

- Implement safeguards to protect Company information according to the sensitivity and potential impact level assigned by the Data Owner.
- Ensure information is protected from unauthorized access, exfiltration, and modification
- Ensure information availability is optimized according to its potential impact rating.

4.11 Workforce

The workforce consists of employees, contractors, consultants, business partners, and other non-employees of the Honest company who have been granted access to Company information and information systems. Responsibilities include:

- Understand and comply with the IT Security policy.
- Complete annual security awareness training
- Understand their role with protecting Company information and ensuring data privacy when required
- Immediately report any observed or suspected security weakness in systems, the network, business processes, physical security in offices and fulfillment centers, or any potential insider threat.

4.12 Third Parties

Make certain all technology systems, services and applications developed for the Honest Company by or in partnership with your company conform to the IT Security policy. Non-conforming systems will not be given permission to deploy on our network.

5.0 Policy

Protection policies are categorized as:

1. Identity, Access, and Entitlement Management
2. Data and Information Protection Management
3. Threat and Vulnerability Management
4. Operations
5. Network, Systems and Applications
6. Cardholder Data
7. People

5.1 Identity, Access and Entitlement Management

5.1.1 Access 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.

5.1.2 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.

5.1.3 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 cost-prohibitive.
- 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

5.1.4 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.

5.1.5 Test Accounts

- Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner, through a formal request to the IT Help Desk via submitting Jira ticket.
- Test accounts must have an expiry date (maximum of 6 months). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approved appropriately.
- Test accounts will be disabled / deleted when they are no longer necessary.

5.1.6 Privileged Accounts

- Privileged account access; ownership, roles and usage must be clearly defined and documented.
- Service accounts used to perform unattended system-to-system or process-to- process authentication must be exclusively used by systems or processes and not by individual users.
- Requirements for elevated privileges, including service accounts, must be approved, documented, and reviewed annually.
- Privileged account access must be restricted to the least privileges necessary to perform job responsibilities and assigned to only those roles that specifically require privileged access.
- Multifactor authentication is required for privileged account, non-console and remote user access.
- Access to all privileged accounts, including super-user, administrative, system accounts, vendor-supplied default accounts, emergency IDs, and interface IDs, must be restricted to appropriate personnel who do not have the responsibility to process business transactions to ensure segregation of duties.
- All system administration or configuration should be conducted using a separate individual privilege account that is different from the administrator’s normal user account used for day-to-day operations.
- All privileged accounts need to be approved by the Director, IT Infrastructure and Operations.

5.1.7 Session Termination and Timeout Controls

To reduce the risk of unauthorized access to company systems and data, controls must be put in place to prevent access to Company terminals or applications while computers are unattended.

- Users must lock their workstation before leaving their computer unattended.
- All systems must be configured to automatically lock, logoff, disconnect, or terminate users sessions after 15 minutes of inactivity. Idle timer for Okta can be extended to one (1) hour given the impact to user productivity and business operations.

5.1.8 Remote Access

- Whenever possible, multi-factor authentication (e.g., Duo, SMS, or Google Authenticator) must be used as an additional layer of protection to authenticate users connecting remotely to Company systems.

5.1.9 Data and Information Protection Management

- All information and information systems must be safeguarded to prevent unauthorized access or modification, misuse, loss, damage, or theft.
- Employees and non-employees with access to non-public information are responsible for protecting Company information from unauthorized access, modification, duplication, destruction, or disclosure whether accidental or intentional. Software, Systems and Service Assurance
- A technology acceptable use policy must be documented and published to employees.

5.2 Information Ownership and Handling

5.2.1 Backup and Information Retentions

Confidential data may be collected or retained for legitimate business purposes only. Refer to the Backup, Retention, and Recovery policy for more details.

- Backup data or media must be stored at a secured off-site location
- Only the minimum amount of confidential information required to conduct business may be collected and retained.
- Business Units must determine whether a legitimate business purpose exists for collection and retention of confidential information.

5.2.2 Information Asset Management

- All information systems must be identified and information about the information system must be maintained in a Company approved asset management/ inventory system.
- This information includes, but is not limited to asset name, asset type, product name, software/hardware vendor, version numbers, current state of deployment, location, and the name of the person or role within the Company responsible for the asset.

5.2.3 Information Disposal

A critical part of safeguarding sensitive information is properly disposing of it when information is no longer needed, its retention period has expired, and information is not required to be retained as directed by the Legal Department and/or pursuant to a Legal Hold.

- Unauthorized destruction or disposal of THC's records or information by an individual may subject the individual to disciplinary action up to and including termination and possible prosecution.
- Information must be disposed of according to the most current publication of NIST SP 800-88 "Guidelines for Media Sanitization."
- In the event a third-party vendor is used to dispose of media, certificates of destruction or sanitation must be provided by the vendor.

5.2.4 Suspected Data Loss or Unauthorized Disclosure

Disclosure of Company information to an unauthorized party, or the suspected loss or disclosure to an unauthorized party, must be reported promptly to the IT Support or Information Security. Refer to the Cybersecurity Incident Response Plan (CSIRP) for more detailed guidelines, processes, and responsibilities.

5.3 Threat and Vulnerability Management

Information systems accessing, transmitting, storing THC information must be protected against malicious or unauthorized programs.

5.3.1 Endpoint Protection

- Endpoint protection software must be deployed on all internet-facing and high-impact servers and all workstations operating on the network.
- Endpoint protection software must be actively running and capable of detecting, removing, and protecting against all known types of malicious software.
- Endpoint protection configurations cannot allow users to disable or alter the software unless specifically authorized by management on a case-by-case basis for a limited time.

5.3.2 Vulnerability Detection

- Vulnerability assessments must be performed regularly on high-impact systems to determine potential business impact by analyzing the type of vulnerability, likelihood, and impact of exploitation.
- Web systems hosting iFrames for payment card transactions must run and pass an Approved Scanning Vendor (ASV) quarterly external vulnerability scan.

5.3.3 Patch Management

All High-impact and internet-facing systems must have critical and high security patches installed within 30 days and conform to the requirements, standards, and guidelines defined in the Patch Management policy.

5.3.4 System and Software Updates

- All High-impact and internet-facing systems must run on a current operating system and on a current version of software based on the vendor' s software currency schedule. Additional requirements and standards are defined in the Patch Management policy.
- In cases where it's financially cost-prohibitive to keep the software at the most current level, compensating controls (e.g., WAF, IDS/IPS, CASB, host-based firewalls, etc.) must be implemented to mitigate risks.

5.3.5 Risk Ranking

All identified vulnerabilities must be evaluated and ranked from highest to lowest risk.

5.4 Infrastructure and Operations

5.4.1 Physical Environmental Security

Company and third-party service providers with access to THC information and information systems must maintain appropriate and adequate physical and environmental controls to protect company information.

- Facilities containing THC information and information assets must be protected from physical intrusion, theft, fire, flood, or other hazards
- Facilities containing THC information and information systems must be constructed in a matter that takes into account the risk of physical and environmental and other potential threats.
- Company and third-party service providers with access to THC information and information systems must deploy physical security measures such as badge readers and video surveillance systems to secure THC data.
- Company and third-party service providers with access to THC information must restrict personnel access based on short-term authorization or job role.
- There must be a process in place to distinguish between employees and visitors. Visitor badges must be surrendered before leaving the facility.

5.4.2 Business Continuity Planning and Disaster Recovery

- Business Units must periodically identify critical information resources used to conduct business and implement actions to minimize impact to business functions from interruptions of information access.
- Technology or Business Support teams must maintain Disaster Recovery Plan (DRP) for High Impact information systems. Plans must be current, tested at least annually and align with the business impact analysis

5.4.3 Change Management

All changes to information systems must follow a formalized, documented, and repeatable change management processes and in conformance with the Change Management policy.

- Changes to information systems must be reviewed, approved, documented, and performed by authorized personnel.
- Segregation of duties in the change control process must be maintained to ensure data integrity, confidentiality and availability are not compromised.

5.4.4 Security Incident Management

- There must be an implemented and formal information security incident management process that clearly defines procedures, roles, and responsibilities.
- Information security incidents must be socialized to appropriate personnel in order to execute the incident management procedures in a timely manner.

5.4.5 Monitoring and Logging

Automation must be implemented to capture and monitor information related to the interaction between users and information assets, and specific events, for the purpose of being able to:

- Reconstruct events
- Establish individual accountability
- Identify security events
- Monitor authentication and authorization events
- Creation and deletion of system level objects
- Monitor unauthorized modification of logs

Audit logs must be generated for all high impact systems and include (where applicable) authentication and authorization logs, server event logs, syslogs, web server logs and firewall logs. Immediate follow up of identified anomalies is required for security events ranked as high or critical. Security controls must be implemented to restrict access to the security logs, as well as, ensure their integrity and availability.

Audit log entries for all system components must at least capture the following details:

- User Identification
- Type of Event
- Date and Time
- Origination of Event

- Identity or name of affected data, system component or resource

5.4.6 Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Satisfactory examples of evidence and compliance include:

- Spot user checks for appropriate access.
- Archival documentation of periodic user access reviews.
- Historical communications on reviews and continuous improvement enhancements.

5.5 Network, Systems and Applications

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the internet as e-commerce, employee internet access through workstations, e-mail access, dedicated connections such as business- to-business, through wireless networks or other sources.

5.5.1 Risk Assessment and Mitigation

Information security risks must be identified and appropriate corresponding controls applied throughout the various phases of the application lifecycle. The phases include software acquisition, development, testing, maintenance and end-of- life.

- A security assessment must be conducted prior to implementation of new software or upon major changes.

5.5.2 Configuration Standards

Secure Configuration Standards must be established, documented and maintained by Information Security. Configuration Standards and the Controls within the standard must be adhered to by system owners. Required Configuration Standards are:

- Firewall and Router Configuration Standard
- System Hardening and Configuration Standard

Configuration Standards must be consistent with a recognized security industry standard such as CIS Benchmark, ISO, or NIST and align with regulatory compliance requirements.

5.5.3 Firewalls and Routers

- Firewalls must be implemented to control computer traffic allowed between the company’s internal network and external untrusted networks as well as to areas handling sensitive information or systems.
- Firewalls should at minimum operate at the network level but also at the application level when the application interfaces with the internet.
- Firewalls and Routers must allow or deny traffic based on business need, meet configuration standards, have documented port and rule sets and follow Change Management procedures when modification is required.
- Firewall traffic must be monitored by the use of an Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS).
- Firewall IDS/IPS systems must be configured to alert personnel of suspected compromises and be maintained with the latest available attacks signatures.

5.5.4 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.

5.5.5 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.

5.5.6 Software Development

- All applications developed for internal or external exposure must be developed in accordance with industry standard secure coding guidelines (e.g. OWASP)
- All developers must be trained in secure coding techniques, including how to avoid common coding vulnerabilities.
- Software Development Lifecycle (SDLC) documentation must contain processes that ensure that applications are developed so they will not be vulnerable to common vulnerabilities (e.g. CSRF, XSS, Injection Flaws, Buffer Overflows, etc.)
- Penetration testing must be performed on Internet-facing and high impact applications or systems at least annually or when major changes are implemented. The must be based on an industry-accepted standard for testing (e.g., NIST SP800-115)

5.5.7 Source Data and Output

- Application source data must be authorized for input, must have a business purpose, and assigned a sensitivity classification.
- Application output must be shared or transmitted in a secure manner and only disclosed to authorized recipients.

5.5.8 Integrity

Application must ensure that transactions are complete, valid and maintain the integrity of data throughout the processing lifecycle.

5.6 Card Holder Data

5.6.1 Card Holder Data Processing and Storage

- Payment card processing and data storage must be outsourced to a contracted PCI DSS compliant service provider and registered on VISA's Global Registry of Service Providers.
- PCI compliance status must be validated prior to onboarding a service provider that will manage, transmit, store cardholder data
- All service providers that manage, transmit or store cardholder data must provide a current PCI DSS Attestation of Compliance (AOC) and are reviewed at least annually.

5.6.2 Card Holder Data Transmission

Strong encryption algorithms and protocols (i.e., TLS, IPSEC, SSH) must be used whenever cardholder data is transmitted or received over open, public networks.

- Only trusted keys or certificates will be accepted
- The data transmission protocol must be implemented to use only secure protocol configurations, and must not support insecure versions or configurations (e.g., use the latest secure TLS and SSH versions only). (PCI DSS Requirement 4.1.b)
- The encryption strength is appropriate for the encryption methodology in use. (PCI DSS Requirement 4.1.b)
- For TLS implementations, TLS must be enabled whenever cardholder data is transmitted or received. (PCI DSS Requirement 4.1.g)
- If SSL or early TLS is used on a POS POI terminal, documentation must be created detailing how it was verified that the terminal is not susceptible to any known exploits for SSL or early versions of TLS. Documentation must include evidence (vendor documentation, system /network configuration details, etc). (PCI DSS Requirement 4.1.h)
- If SSL or early TLS is used anywhere but a POS POI terminal, a risk mitigation and migration plan must be created, which includes the following: (PCI DSS Requirement 4.1.h)

Access assigned to individual personnel is based on their job classification and function. (PCI DSS Requirement 7.1.3). An authorization form specifying all required access privileges is required and must be generated and signed by management approving the access. (PCI DSS Requirement 7.1.4)

5.7 Third-Party Service Provider Review

Careful consideration must be taken to evaluate third-party service providers hosting critical business that house and/or process restricted data, especially those within the scope of Sarbanes-Oxley and PCI, before being on-boarded and annually to ensure they are secure, available, and operating accurately.

- Both technical and security assessments must be conducted prior to on-boarding the service provider to determine compatibility with existing technical standards and compliance with security policies
- Evidence of the most recent Disaster Recovery Plan and Testing along with SOC1 reports must be obtained and reviewed on an annual basis to identify any issues and verify alignment with existing Company security policies

5.8 People

Employees must protect Company information and the information systems they use to process, store, or transmit Company information. Violations of these policies and standards or potential information security incidents must be reported to Management.

Failure to comply with the IT Security policy may result in disciplinary actions up to and including termination of employment for employees or termination of contracts for third-party service providers.

5.8.1 Security Awareness Training

- Annual information security awareness training must be provided to all employees and non-employees with access to non-public information.
- The information security awareness training must be based on The Honest Company's IT Security policy and relevant legal and regulatory requirements.

5.9 Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Satisfactory examples of evidence and compliance include:

- Spot user checks for appropriate access.
- Archival documentation of periodic user access reviews.
- Historical communications on reviews and continuous improvement enhancements.

6.0 Enforcement

All Company personnel found in policy violation may be subject to disciplinary action, up to and including termination. Access will be revoked for all contractors, consultants, vendors, or business partners found in violation of this policy.

7.0 Resources and References (internal and external)

FIPS Publication 200

NIST Special Publication 800-53 Revision 5

Backup, Retention, and Recovery Policy

Change Management Policy

Cybersecurity Incident Response Plan (CSIRP)

Disaster Recovery Plan

User Access Review Process

New Hire Standards