Honest Company, Inc.

Internal Information Protection Policies and Standards

Version and Revision

Version	1.4
Document Owner	Nicole Holmes, Director, Information Security
Effective Date	September 1, 2018
Next Review Date	June 1, 2019
Comply By Date	September 1, 2019

Revision

The Internal Information Protection Policies and Standards will be reviewed under the supervision of the Director of Information Security when the following events occur:

- Required Annual Review
- Legal and Regulatory Changes
- Major changes to Business Operations
- Major Security Event
- Changes to Information Security Best Practice

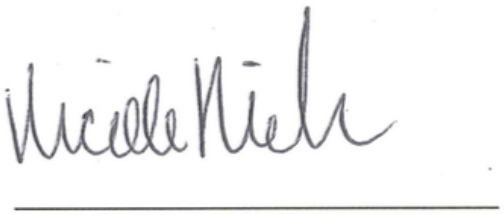
Comply By Date

The policies and standards contained herein are either currently in place or will be by the stated "Comply By Date" above. Policies and Standards can be modified at any time at the Company's discretion.

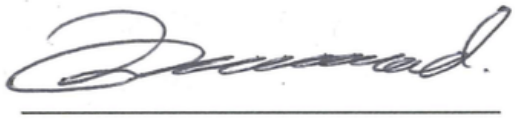
Table of Contents

Authority

We support the information protection policies and standards outlined in this document and those required by law and regulation. We expect all measures are implemented and followed consistently.

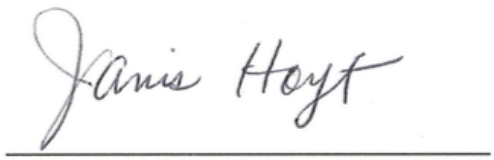


Nicole Miller
General Counsel

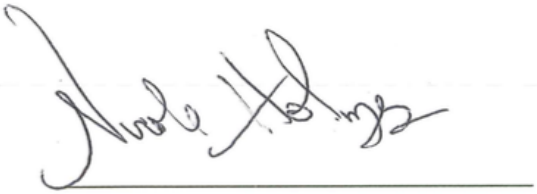


Muhammad Shahzad
Chief Financial Officer

Bob Van Dusen
Vice President, Information Technology



Janis Hoyt
Chief People Officer



Nicole Holmes
Director, Information Security

Introduction

The primary mission of Information Security is to protect The Honest Company ("Company") brand and key 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 Security Management.

Scope and Policy

Scope

The Honest Company's Internal Information Protection Policies and Standards (IIPPS) applies to all systems, employees and non-employees that have been granted access to The Honest Company network, information or information systems.

Policy Statement

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

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.

Regulation

The Information Protection Policies and Standards 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:

- 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

Roles and Responsibilities

Chief Financial Officer, VP of Technology

Responsible for oversight and support the Information Protection Policies and Standards. Reviews and approves policies and ensures alignment at the senior leadership level. Has overall accountability to meeting the IIPPS mandates.

General Counsel

Responsible for ensuring the information security and information technology programs are aligned with legal and regulatory requirements.

Information Security Director

The Information Security Director is responsible for the development and maintenance of the Information Protection Policies and Standards. Policies are reviewed and approved by the CFO, General Counsel and VP of IT. Standards are approved by the Director of Information Security. Additional responsibilities 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

Security Architects

Security Architects are responsible for designing and implementing information security systems and solutions that adhere to IIPPS policies and aim to better secure Company information and systems. Additional responsibilities include:

- 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

Security Operations

Security Operations resources are responsible for daily activities related to monitoring, maintaining, assessing and defending security and information systems. They monitor compliance of the security policy and standards.

Security Operations is a key component to incident response execution, planning and testing.

After major environmental changes or a significant security incident, Security Operations will provide feedback and request any necessary changes to the security controls or standards.

Human Resources

Human Resources is responsible for ensuring the Employee Handbook references the Information Protection Policies and Standards. HR will conduct background checks to ensure employees are properly vetted before they are permitted to access information assets belonging to the Company as well as direct that all Company property be returned upon employee's separation from the Company. Third party employment agencies shall perform their own background checks for relevant resources.

Managers

People managers are responsible to manage risks to information and information systems by ensuring information protection policies are understood and implemented in their respective functional areas. Additional responsibilities include:

- 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

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 include:

- Understand the Information Protection Policies and Standards requirements for their area of responsibility
- Ensure the technology they are responsible for is securely deployed with the appropriate security controls and in conformance with the IIPPS
- 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 IIPPS
- Application development roles must complete secure coding training at least annually
- Privileged users that handle Restricted data must ensure information is stored in a secure place and accessed only according to security controls detailed herein

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:

- Assign sensitivity level and classify data they are responsible for as Restricted, Internal or Public
- In partnership with the Data Custodian (technology personnel), ensure data classified as Public, Internal or Restricted is maintained at the appropriate confidentiality, integrity and availability level

- Ensure access to data is based on job role and is aligned with the policies of least privilege and need-to-know

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

Workforce and Contingent Workers

The workforce consists of employees and Contingent Workers including authorized non-employees (e.g. temporary workers, consultants, contractors, etc.) of the Company who have been permitted access to Company information, and information systems. Responsibilities include:

- Understand and implement the Internal Information Protection Policies and Standards
- If working with non-public business data and/or issued Company property, complete annual security awareness training
- Understand their role with protecting Company information and ensure 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

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 Internal Information Protection Policies and Standards document. Non-conforming systems will not be given permission to deploy on the Company's network.

Protection Policies

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

1 Identity, Access and Entitlement Management

1.1 Access Management

1.1.1 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 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
- Access rights must be reviewed periodically using a formal process to ensure user accounts are still required, are authorized and have proper access rights
- A formal process must be in place for revoking or transferring user access to all Company information and information systems

1.1.2 Access control systems must be set to a default "deny-all" setting

1.2 Third Party Access

1.2.1 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 the Company's information systems and/or non-public information.

1.2.2 Contracts with non-employees who obtain access to Company non-public information or information systems and contracts with such individuals' employers must require compliance with relevant Company information security requirements.

1.2.3 Access for non-employees must only be activated or extended after supervisor and legal or HR approval.

1.2.4 Access for non-employees must be assigned a termination date in the access control system and must not exceed one year. Subject to approved extensions per 1.2.3.

1.2.5 Only activate remote-access technologies for vendors and business partners when needed and immediately deactivate remote-access sessions after use.

1.3 User Accounts

1.3.1 All systems containing non-public information are required to utilize at least an account ID and password/PIN combination authentication mechanism.

1.3.2 Unique IDs must used for all user-level access. Shared and generic accounts are not permitted.

1.3.3 Access must be immediately revoked for all terminated users.

1.3.4 Inactive user accounts must be deactivated if not in use longer than 90 days

1.3.5 Deactivated accounts must be deleted from the access control system after 90 days.

1.3.6 Administrators must verify the user identity before modifying credentials.

1.3.7 Administrators must not use user-level credentials for privileged access.

1.3.8 All user accounts must have identifiable owner.

1.4 User Authentication

1.4.1 Strong cryptography must be used for transmission of authentication credentials

1.4.2 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).

1.4.3 User accounts must be locked out after six failed login attempts

1.4.4 User account lockout duration must be set to a minimum of 30 minutes or until an administrator unlocks the account.

1.4.5 Passwords or pass-phrases are required to be a minimum length of 8 characters and contain both numbers and special characters.

1.4.6 Passwords or pass-phrases must be changed at least every 90 days.

1.4.7 The last four passwords or pass-phrases must not reused.

1.4.8 Remote-access technologies in use must automatically disconnect sessions after a specific period of inactivity

1.5 User Authorization

1.5.1 All systems containing non-public information are required to follow a role-based access model where entitlements are based on job duties, least privileged and need-to-know controls.

1.6 Privileged Accounts

1.6.1 Privileged or administrator 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

1.6.2 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.

1.6.3 Multifactor authentication is required for privileged account, non-console and remote user access. User authentication for Privileged Accounts requires two of the following: (a) something you know (e.g. password); (b) something you have (e.g. token) or ; (c) something you are (e.g. biometric).

1.6.4 Privileged account entitlements and access must be assigned by job role

1.6.5 All privileged account access must have documented approval from a supervisor and the system owners or support teams.

1.6.6 Privileged accounts must use designated administrator-level credentials for administrative tasks.

1.6.7 All Privileged accounts must have an identifiable owner.

1.7 Password and Pin Management

1.7.1 At least a password or other similar mechanism must be used to authenticate the identity of the user or entity prior to accessing Company information systems containing non-public information.

1.8 Account Lockout, Session Termination and Timeout Controls

1.8.1 Account lockout controls, session timeout controls, and session termination controls must be implemented on all information systems.

2 Data and Information Protection Management

2.1 Information Protection

2.1.1 All information and information systems must be safeguarded to prevent unauthorized access or modification, misuse, loss, damage or theft .

2.1.2 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.

2.1.3 A Technology Acceptable Use policy must be documented and published to employees.

2.1.4 Company-issued laptops, mobile devices and external storage devices that are lost or stolen must be reported to the Information Security team immediately.

2.2 Information Ownership and Handling

2.2.1 All Company information and information systems must have clear ownership and must be managed appropriately.

- Information Owners must be designated for all Company information and information systems.
- The Information Owner must determine the classification of information and to reclassify information when warranted

2.2.2 All Company information must be stored only on Company workstations, servers, databases, software or within approved third-party systems managed by approved contractually bound service providers.

2.3 Information Classification

2.3.1 All Company information must be classified according to its value, sensitivity and criticality.

Public	Information that can be made available to the general public through approved Company channels. Unauthorized disclosure or alteration of the data will result in little or no adverse effect to the Company. Information is this category is not protected by regulatory or compliance mandates and is not confidential to the Company.

Internal	Information that is utilized by the Company and not intended for the public. Access to this data is restricted to authorized personnel based on department, job role or management approval. Unauthorized disclosure or alteration of the data could result in moderate risk to the Company.

Restricted	Information that is confidential, highly compartmentalized, protected by regulation, policies, Company contracts or is proprietary to the Company. Unauthorized disclosure or alteration of the data could result in serious adverse effects to the Company.

2.4 Information Retention

2.4.1 Company data may be collected or retained for legitimate business purposes only and subject to a written retention policy.

- Managers must determine whether a legitimate business purpose exists for collection and retention of Company data
- Records and information must be retained if: (1) according to the Records Retention Schedule, as referenced in Appendix A, the retention period has not expired; or (2) if you have been instructed to do so by the Legal Department

2.5 Backup

2.5.1 Information must be periodically backed up according to its potential impact to the company. Potential impact levels assigned are high, moderate or low in each of the security objectives (confidentiality, integrity, availability).

2.5.2 Backup data or media must be stored in a secure off-site location.

2.6 Information Asset Management

2.6.1 All information systems must be identified and information about the information system must be maintained in a Company approved asset management/ inventory system.

2.6.2 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.

2.7 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.

2.7.1 Unauthorized destruction or disposal of Company records or information by an individual may subject the individual to disciplinary action up to and including termination.

2.7.2 Information must be disposed of according to the Data Sanitization Standards, as referenced in Appendix A.

2.8 Suspected Data Loss or Unauthorized Disclosure

2.8.1 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 teams.

3 Threat and Vulnerability Management

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

3.1 Antivirus

3.1.1 Antivirus software or an equivalent must be deployed on all internet-facing and high-impact servers and all workstations operating on the network.

3.1.2 Antivirus software or an equivalent must be actively running and capable of detecting, removing, and protecting against all known types of malicious software.

3.1.3 Antivirus software or an equivalent must be capable of generating audit logs and audit logs must be retained for one year

3.1.4 Antivirus 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.

3.2 Vulnerability Detection

3.2.1 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.

3.2.2 Web systems hosting iframes for payment card transactions must run and pass an Approved Scanning Vendor (ASV) quarterly external vulnerability scan.

3.3 Patch Management

3.3.1 All High-impact and internet-facing systems must have critical and high security patches installed within 30 calendar days

3.4 System and Software Updates

3.4.1 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.

3.5 Risk Ranking

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

4 Infrastructure and Operations

4.1 Physical Environmental Security

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

- Facilities containing Company information and information systems must be protected from physical intrusion, theft, fire, flood or other hazards
- Facilities containing Company information and information systems must be constructed and located accounting for the risk of physical and environmental threats and other potential threats.

4.1.2 Company and authorized third-party service providers with access to Company information and information systems must use security systems such as a badge reader and video surveillance to manage access control.

4.1.3 Company and third party service providers with access to Company information must restrict personnel access based on short-term authorization or job role.

4.1.4 There must be a process in place to distinguish between employees and visitors. Visitor badges must be surrendered before leaving the facility.

4.2 Business Continuity Planning and Disaster Recovery

4.2.1 Departments must periodically identify critical information resources used to conduct business and implement actions to minimize impact to business functions from interruptions of information access.

4.2.2 Technology or Business Support teams must maintain Disaster recovery ("DR") plans for High Impact information systems. Plans must be current, tested at least annually and align with the business impact analysis.

4.3 Change Management

4.3.1 All changes to information systems must follow a formalized, documented, and repeatable change management processes.

- 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

4.4 Incident Management

4.4.1 There must be a documented and formal information security incident management process that clearly defines procedures, roles and responsibilities.

4.4.2 Information security incidents must be communicated to appropriate personnel in order to execute the incident management procedures in a timely manner.

4.5 Risk Management

4.5.1 A formal risk assessment process must be implemented and documented.

4.5.2 A formal risk assessment must be conducted at least annually or upon major change to the environment.

4.5.3 The risk assessment must leverage an industry standard framework such as National Institute of Standards and Technology (NIST).

4.5.3 The risk assessment identifies critical assets, threats, and vulnerabilities.

4.6 Monitoring and Logging

4.6.1 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

4.6.2 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

4.6.3 Audit log entries for all system components must at least capture:

- User Identification
- Type of Event
- Date and Time
- Origination of Event
- Identity or name of affected data, system component or resource

4.6.4 Audit logs must be reviewed daily to identify anomalies or suspicious activity

4.6.5 Immediate follow up of identified anomalies is required for security events ranked as high or critical.

4.6.6 Audit logs for high impact systems must be retained for at least one year with three months immediate available for analysis.

4.6.7 Maximum availability must be maintained for systems critical to security control.

5 Network, Systems and Applications

All systems must be reasonably 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.

5.1 Risk Assessment and Mitigation

5.1.1 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.

5.2 Configuration Standards

5.2.1 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

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

5.3 Firewalls and Routers

5.3.1 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.

5.3.2 Firewalls should at minimum operate at the network level but also at the application level when the application interfaces with the internet.

5.3.3 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.

5.3.4 Firewall traffic must be monitored by the use of an Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS).

5.3.5 Firewall IDS/IPS systems must be configured to alert personnel of suspected compromises and be maintained with the latest available attacks signatures.

5.4 Wireless Company Network Devices

5.4.1 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.

5.4.2 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 System Access, Passwords and Security Parameters

5.5.1 Only authorized or approved devices may be used to access, store or process non-public information.

5.5.2 All network connections must be documented, centrally managed, properly secured, approved and periodically audited.

5.5.3 Remote access must be limited to authorized users and only allowed through the Company approved mechanisms.

5.5.4 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.).

5.5.6 All unnecessary default accounts must be removed or disabled before installing the device onto the network.

5.5.7 The encryption keys, passwords or pass-phrases must be changed at least annually or anytime anyone with knowledge of the credentials leaves the company or moves to a position that no longer requires knowledge of the credentials.

5.5.8 All encryption keys utilized must be securely distributed and stored.

5.5.9 Strong cryptography (i.e. SSH, VPN, TLS 1.2) must be used for any non-console or web-based management interface used for administration of systems or system components.

5.5.10 Separation of duties must be in place between personnel working in the development/test environment and those working in production environments.

5.6 Software Development

5.6.1 All applications developed for internal or external exposure must be developed in accordance with industry standard secure coding guidelines (e.g. Open Web Application Security Project (OWASP))

5.6.2 All developers must be trained in secure coding techniques, including how to avoid common coding vulnerabilities at least annually.

5.6.3 Software Development Lifecycle (SDLC) documentation must contain processes that ensure applications are developed so they will not be vulnerable to common vulnerabilities (e.g. CSRF, XSS, Injection Flaws, Buffer Overflows, etc)

5.6.4 Penetration testing must be performed on Internet-facing and high impact systems at least annually or when major changes are implemented. The testing must be based on an industry-accepted standard for testing (e.g NIST SP 800-115)

5.7 Source Data and Output

5.7.1 Application source data must be authorized for input, must have a business purpose and assigned a sensitivity classification.

5.7.2 Application output must be shared or transmitted in a secure manner and only disclosed to authorized recipients.

5.8 Integrity

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

6 Cardholder Data

6.1 Cardholder Data Processing and Storage

6.1.1 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.

6.1.2 The company's Service Provider Compliance Validation Procedures must be followed prior to on-boarding a service provider that will manage, transmit, store cardholder data.

6.2.3 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.

6.2 Cardholder Data Transmission

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

Controls:

- 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)

7 People

Employees must protect non-public 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 IIPPS may result in disciplinary actions up to and including termination of employment for Employees or termination of contracts for third party service providers and Contingent Workers.

The Company may, in its sole discretion, utilize whatever form of discipline is deemed appropriate under the circumstances, up to, and including, termination of employment. The Company's policy of discipline in no way limits or alters the "at-will" employment relationship.

7.1 Security Awareness Training

7.1.1 Annual information security awareness training must be provided to all employees and non-employees with access to non-public information.

7.1.2 The information security awareness training must be based on the Company's Internal Information Protection Policies and Standards and relevant legal and regulatory requirements.

7.2 Secure Coding Training

7.2.1 Annual secure coding training must be provided to all employees and no-employees that have job roles that perform software developer functions.

7.2.2 The secure coding training must be based on Open Web Application Security Project (OWASP) practices.

7.3 Tampering

7.3.1 Information Security tools that reside on Company assets must not be removed or modified without the prior approval of the Information Security team.

Exceptions

Meeting policy requirements are not always easily met. There are acceptable business and technological justifications that will warrant an exception to the policy. Exceptions must be documented and approved by the signers of the IIPPS.

Resources and References

Appendix A

References

FIPS Publication 200

NIST Special Publication 800-53 Revision 4

Supporting Documents

The Supporting documents set forth below are incorporated herein by reference.

Document Name	Description	Location Link
Firewall and Router Configuration Standards	Standards to ensure rule sets for firewalls and routers are meet minimum security baselines	TBD
System Hardening and Configuration Standards	Standards to ensure system components are properly secured, vendor defaults are changed and only authorized programs are running.	TBD
Data Classification & Retention Policy and Procedures	A framework to ensure sensitive information is handled according to the risk it poses to the organization. It also supports regulatory requirements for maintaining data privacy.	Information Classification and Records Management Confluence Page
Data Classification and Retention Schedule	List of records by department with their associated sensitivity level, storage location and owner info	Information Classification and Records Management Confluence Page
Data Sanitization Standards	Standards to ensure confidentiality is maintained by properly disposing of data	Information Classification and Records Management Confluence Page
Vulnerability Discovery and Risk Ranking Process	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.	Vulnerability Scan Overview
Software Development Life Cycle (SDLC) Process	Confluence page that explains the SDLC process	SDLC Confluence Page
Security Awareness Training Process	A program to educate users with their roles and responsibilities to ensure the confidentiality, integrity and availability of company information is maintained.	Security Awareness
Service Provider Compliance Validation Process	Establishes procedures around the selection of and ongoing validation of service providers	Service Provider Evaluation Process

Document Name	Description	Location Link
Cyber Security Incident Response Plan CSIRP	Actionable guideline to address cybersecurity and information security incidents that effect critical infrastructure and assets	CSIRP
Computer Policy	Technology Acceptable Use Policy included as part of the Employee Handbook	Computer Policy - Employee Handbook
Change Management	Process to ensure IT and business activities are aligned and continue to be aligned with optimal efficiency, minimal disruption, re-work and risk.	Change Management Process