INFORMATION SECURITY POLICY

DEPARTMENT ISSUING POLICY: CYBERSECURITY

POLICY OWNER: CHIEF INFORMATION SECURITY OFFICER

Table of Contents

Information Security Approvers

Approver Title	Approver Name	Date Approved	Approver Signature
CISO	Rich Agostino	9/29/2021	Email Approval
CISO	Rich Agostino	4/26/2021	Email Approval
CISO	Rich Agostino	9/28/2020	Email Approval
CISO	Rich Agostino	10/7/2019	Email Approval
CISO	Rich Agostino	4/18/2019	Email Approval
CISO	Rich Agostino	9/27/2018	Email Approval
CISO	Rich Agostino	05/08/2018	Email Approval
Senior Director	Jodie Kautt	01/22/2018	Email Approval

Information Security Revision History

Date of Revision	Revision Version	Revision Author	Brief Revision Description
9/23/2021	15.0	Francois Barnard	Minor updates and clarifications
4/30/2021	14.0	Francois Barnard	Updated the domains with specific focus on change management, secure delivery and logging
9/25/2020	13.0	Francois Barnard	Updated most domains with a specific focus on IAM, Vulnerability Management, SAST, DAST and Configuration Management
9/5/2019	12.0	Erin Getty	Updated language in Intro. Updated grammar and format in IAM, Secure Delivery, IT Operations, Threat and Incident Management, Third-Party Security, Disaster Recovery; added Definitions
4/8/2019	11.0	Erin Getty	Updated IAM, Secure Delivery, Threat and Incident Management, and Definitions
8/15/2018	10.5	Erin Getty	Reordered the domains, large updates to IAM and Secure Delivery, definition updates
04/24/2018	10.4	Erin Getty	Update to all domains, definition updates
01/31/2018	10.3	Erin Getty	Clarification of language in Secure Delivery, Identity and Access Management, Threat Management, and Network Security

Purpose

The Information Security Policy ("Policy") provides detailed statements of practices and capabilities that must be in place to ensure the confidentiality, integrity and availability of Target's information resources and information assets.

Authority and Oversight

The Risk and Compliance Committee of the Target Board of Directors (the "Board") authorized the establishment of an enterprise-wide Program, including oversight of the development, implementation and maintenance of the Program, and assignment of specific responsibilities for implementation and reviewing of reports from management. This Policy is one of the products of the Program, both of which are designed and managed by the Chief information Security Officer ("CISO"). The CISO reviews and approves the Policy at least annually.

Scope

The Policy applies to the information assets and resources handled or maintained by Target team members and contractors, and to information assets and resources handled or maintained by Target's subsidiaries, affiliates and third parties. Just like the Acceptable Use of Information Resources Policy, team members and contractors must comply with this Policy. Team members who violate this Policy may be subject to disciplinary action, up to and including immediate termination. Contractors who fail to comply with this Policy may find their ongoing assignment with Target affected. Violators may also be subject to legal action, including criminal prosecution, and Target reserves the right to take any other action it believes is appropriate.

Definitions

For a list of definitions, please refer to Appendix A of this document.

Structure and Maintenance

The Policy is based on industry-accepted security frameworks and applicable federal, state, and international regulations and obligations. It is formatted and customized to meet Target's business needs. Additionally, the Policy is reviewed annually and revised, as needed, to address changes in security risks due to changes in Target's technology, business needs, and emerging threats.

Roles and Responsibilities

Business unit management – responsible for the establishing and maintaining the security of the information and information resources used by team members and contractors within their teams and for ensuring their teams understand how to comply with the information security requirements. Business unit management is responsible for documenting and maintaining daily operational procedures for its products and/or services.

Information Systems Owner – responsible for managing the risks associated with their Information Systems, including monitoring, and enforcing the security requirements defined for their Information Systems.

Relationship Manager – responsible for managing the risks associated with the vendor, including monitoring, remediation of findings and enforcing Vendor adherence to Target's operational and policy requirements.

Team members and contractors – responsible for understanding the information security requirements and consistently applying them in their work activities, completing all information security training as required by their role or assignment, and using daily operational procedures to support compliance, where applicable.

Variance and Exception

If you are unable to comply with information security requirements, or if you are aware of a situation that may be a security risk to Target, you must report it by contacting security@target.com.

If you would like to remain anonymous, you may contact the Integrity Hotline at 1-800-541-6838 (individuals in U.S.); 000-800-100-1657 (individuals in India); 470-219-7116 (individuals in other non-U.S. locations); or report online at Integrity at Target.

Resources

Engage your Business Information Security Officer (BISO) for assistance in complying with this Policy.
Implementation Guidance – keep in mind that the Policy provides the requirements that must be met, but it rarely provides information on how to meet it because there might be multiple ways to do so. In addition to working with your BISO, find guidance on implementing the information security requirements in the Product Security Portal.

Requirements

Asset Management and Data Protection

Scope: Overall management of tangible and intangible assets, including controls to protect data on such assets.

Asset Management

Asset Owners (CS-1557053)

Identify owners (team or individual) for IT hardware and software assets and information assets. Owner responsibilities include, but are not limited to, the following:

Low	Med	High	Requirements
X	X	X	Accountability for security risks associated with assets.

Inventory of Assets (CS-1557054)

Implement a system or procedures to identify, track, label, and maintain an inventory of assets. Implement mechanisms as appropriate, to assist in maintaining an up-to-date inventory of information system components. . Identify, track and maintain the following items:

Low	Med	High	Requirements
X	X	X	Asset name, Asset control ID or serial number, physical location, Product, Product Group, Portfolio, Environment (test, stage, production, etc.), asset category, operating system or application version.

Data Management

Secure Distribution of Media (CS-1557055)

Ensure secure distribution of media by performing the following:

Low	Med	High	Requirements
	X	X	Media that contains SHR, Guest PI, or PHI information must be physically secured.
		X	The incoming/outgoing distribution of SHR media must be recorded and approved by the data owner prior to moving the media.
		X	Media that contains SHR data must be sent by secured courier or other delivery method that can be accurately tracked.
		X	For systems in scope for PCI: All removable media must be labeled as SHR and approval must be obtained prior to moving the data from secure areas. The removable media must be recorded within an inventory of media assets.
		X	Media that contains SHR data must be encrypted before it is physically distributed.

Protect Payment Card Account Information (CS-1557056)

Ensure that Primary Account Number (PAN) is protected from unauthorized access.

Low	Med	High	Requirements
		X	For PCI systems only, allow only authorized personnel with a legitimate business need to see full or untruncated branded payment card Primary Account Number (PAN). Render branded payment card PAN unreadable for those that do not have a business need to access. Where hashed and truncated versions of the same PAN are present, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.
		X	For systems in scope for PCI: The branded payment card Primary Account Number (PAN) must be unreadable to those who do not have a business need to access the data.
		X	For systems in scope for PCI: The Primary Account Number (PAN) data must be stored and appropriately protected in such a way that the original PAN cannot be reconstructed.

Protect Payment Card Data (CS-1557057)

Implement controls to protect Payment Card data as follows:

Low	Med	High	Requirements
		X	For systems in scope for PCI: The card verification security code printed on a branded payment card must only be accessed prior to the authorization of the transaction. The card verification security code must not be stored or transmitted after the transaction has been authorized.
		X	For systems in scope for PCI: The following card holder data are not permitted to be retained or stored: • Full track contents from the magnetic stripe located on the back of a card, contained in a chip, or elsewhere • Card verification code or value storage • Personal identification number (PIN) • Encrypted PIN block storage
		X	For systems in scope for PCI: The Sensitive Authentication Data (SAD) stored electronically on a branded card must only be accessed prior to the authorization of a transaction. The SAD data is not allowed to be stored or transmitted after the transaction has been authorized.
		X	For systems in scope for PCI: Card data is not allowed to be stored on systems that are publicly accessible.

Metadata Attributes (CS-1557059)

Ensure Guest data is properly attributed.

Low	Med	High	Requirements
	X	X	Product teams who produce data, or own or support products that produce data, must implement and maintain the appropriate meta data attributes as prescribed in the Data Management Policy.

Target Information in a Shared Location (CS-1557060)

Ensure segregation of Target data.

Low	Med	High	Requirements
	X	X	Target information must be logically or physically segregated from non-Target information when stored in a shared location.

Records and Information Asset Retention and Disposal

Records Retention (CS-1557061)

Ensure retention of records and data complies with legal requirements and internal policy.

Low	Med	High	Requirements
X	X	X	The retention of records and information assets must be limited in accordance with the Records and Information Management Policy and Records Retention Schedules.
		X	For systems in scope for PCI: Information System Owners must at least quarterly, identify and delete any cardholder data or information that exceeds the retention period defined in the Records Retention Schedule.

Secure Disposal of Media (CS-1557062)

Ensure secure disposal.

Low	Med	High	Requirements
X	X	X	The information contained on removable media must be appropriately protected by either physically destroying the media prior to distribution outside of Target, or by securely disposing (e.g., degauss, overwrite, wipe) of the information prior to reuse.
	X	X	Paper documents that contain Confidential or SHR information must be disposed of by shredding, by placing them in Target secure disposal containers, or by using a Target approved information destruction vendor.

Data Encryption and Key Management

Encrypting in Transit (CS-1557063)

Encrypt or equally and appropriately protect sensitive information in transit.

Low	Med	High	Requirements
X	X	X	Remote administrative access must occur over a secured encrypted channel.
	X	X	Confidential and SHR information must be encrypted or equally and appropriately protected when transmitting or distributing it electronically over a public network.
		X	SHR information must be encrypted or equally and appropriately protected when transmitting or distributing it electronically over internal Target networks.

Encrypting Information at Rest (CS-1557064)

Encrypt or equally and appropriately protect sensitive information at rest.

Low	Med	High	Requirements
		X	SHR information must be encrypted or equally and appropriately protected when stored.

Managing Cryptographic Keys (CS-1557065)

Securely manage cryptographic keys.

Low	Med	High	Requirements
X	X	X	Strong cryptographic keys must be generated.
X	X	X	Cryptographic keys must be securely distributed.
X	X	X	Cryptographic keys must be rotated upon expiration.
X	X	X	Cryptographic keys must be revoked and replaced if the integrity of the keys have been weakened or if the keys are suspected of being compromised.
X	X	X	Cryptographic keys that are replaced, must be appropriately archived or destroyed.
X	X	X	Cryptographic keys must be securely stored and appropriately protected against unauthorized substitution.
X	X	X	Cryptographic key custodians must be established and they are required to formally acknowledge that they understand and accept the key-custodian responsibilities.
X	X	X	If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (e.g., requiring two or three people, each knowing only their own key component, to reconstruct the whole key).

Managing Cryptographic Keys (CS-1557065) - continued

Securely manage cryptographic keys.

Low	Med	High	Requirements
		X	For systems in scope for PCI: • Any keys used to secure cardholder data must be protected against disclosure or misuse. Key-encrypting keys used to protect data encrypting keys must be at least as strong as the data-encrypting key. Access to cryptographic keys must be limited to the fewest number of custodians necessary and the cryptographic keys must be securely stored in the fewest possible locations and forms • Only authorized personnel with a legitimate need must be allowed to see the full or untruncated branded payment card Primary Account Number (PAN) • The branded payment card Primary Account Number (PAN) must be unreadable to those who do not have a business need to access the data • The Primary Account Number (PAN) data must be stored and appropriately protected in such a way that the original PAN cannot be reconstructed

Certificate Management (CS-1557066)

When using cryptographic certificates, use Target-approved methods to ensure certificates are securely managed. Only approved Target Root Certificate Authorities (CA) or members of Target-approved public CA root programs are considered trusted roots.

Low	Med	High	Requirements
X	X	X	Only Target-approved Certificate Authority (CA) must be used to sign certificates.
X	X	X	Internally signed certificates must not be exposed to external networks.
X	X	X	Wildcard or Subject Alternative Name (SAN) certificates must be managed in accordance with Target Certificate generation guidance.
X	X	X	Certificates must be revoked and replaced when the integrity of the private key or Certificate Authority has been weakened or compromised.
X	X	X	Certificates that are replaced, must be appropriately archived and/or destroyed.

Cryptographic Solutions (CS-1557067)

Establish secure solutions for Target-approved cryptography.

Low	Med	High	Requirements
X	X	X	Strong cryptographic algorithms and key lengths must be used using industry best practices (e.g., NIST Cyber Security Framework, FIPS).
X	X	X	The root Certificate Authority, the policy Certificate Authority, and the issuing Certificate Authority private keys must be stored in a Hardware Security Module (HSM).
X	X	X	The DCCS team (Digital Certificates and Cryptographic Services) must document and maintain the key revocation information.
X	X	X	The DCCS team (Digital Certificates and Cryptographic Services) must document and maintain information related to their services, including the Key Policy and Certification Practice Statement.

Identity and Access Management

Scope: Overall management of digital identities, user accounts, non-user accounts and access to provide the right level of resources to the right individuals, devices, and processes through appropriate channels.

Authentication Management

User Identification and Authentication (CS-1557069)

Ensure secure user identification and authentication by performing the following:

Low	Med	High	Requirements
X	X	X	Each user must be assigned a unique identifier to ensure that system activities can be traced back to the responsible user. The unique identifier must be maintained in an approved system of record.
X	X	X	External connections to Target network must utilize strong authentication.
X	X	X	Privileged access to Target's network must utilize strong authentication.
X	X	X	The identity of the requestor must be verified prior to processing a password change request.
X	X	X	User and non-user accounts must utilize Target's approved authentication service prior to being granted access to authorized resources/functions.
		X	All externally accessible non-guest facing applications must utilize strong authentication for users.
		X	For systems in scope for PCI: Privileged Application access must utilize multi-factor authentication.

Restrictions for Interactive Non-User Accounts (CS-1557070)

Restrict interactive non-user accounts (e.g., testing, training, checkout accounts) and passwords as follows:

Low	Med	High	Requirements
X	X	X	Interactive non-user accounts used for testing and training with access to production systems or data must reset/change passwords, or lock after the completion of the training class or testing cycle not to exceed 1 week in duration. If the testing or training account has access to SHR or Confidential information, the duration must not exceed 48 hours.

Restrictions for Non-Interactive Non-User Accounts (CS-1557071)

Restrict non-interactive, non-user accounts (e.g., system, database, application) and passwords as follows:

Low	Med	High	Requirements
X	X	X	Non-interactive non-user accounts are single-purpose accounts that must not be shared across teams, platforms, environments or applications.

Restrictions for Database Access (CS-1557072)

Restrict database access as follows:

Low	Med	High	Requirements
X	X	X	The Information System Owner must ensure that authentication and authorization is enabled and used to gain access to any database supporting their system/application.
X	X	X	Non-user accounts used to connect applications to databases are single-purpose accounts and must not be shared across teams, platforms, environments or applications.
		X	For systems in scope for PCI: Only the database administrator is allowed to directly access or query the database.
	X	X	For systems in scope for PCI, HIPAA, GLBA or SOX, and systems with SHR data: User and non-user accounts must utilize Target's approved authentication service prior to being granted access to authorized resources/functions.

Restrictions for Third-Party Remote Access (CS-1557073)

Manage and restrict third-party remote access as follows:

Low	Med	High	Requirements
X	X	X	Access must only be enabled for the time period needed and must be disabled when the third-party engagement or contract has ended.
		X	For systems in scope for PCI: Information System Owners must monitor access to ensure that third parties are only accessing authorized systems and information and only during approved timeframes.

Public and Private Key Pair Management (CS-21956874)

The private keys used for authentication must be managed as a secret.

Low	Med	High	Requirements
X	X	X	Private keys must not be shared between users.
X	X	X	Private keys must be appropriately protected from unauthorized access.
X	X	X	Private keys for user and non-user accounts must not be copied, moved or stored on another device.
X	X	X	Private keys for user and non-user accounts must be stored in an approved enterprise secrets management tool.

Identity and Access Management Configuration

Identity and Access Management Configuration (CS-1557074)

Configure identity and access management controls into systems:

Low	Med	High	Requirements
X	X	X	Initial, temporary passwords must be invalidated after forcing the user to set up a new password at the first use.
X	X	X	Non-Guest facing Target issued devices must lock and require user re-authentication of the device after 15 minutes of inactivity.
X	X	X	Business applications that are publicly accessible must require user re-authentication after 60 minutes of inactivity. Internally accessible applications must require user re-authentication after 240 minutes of inactivity.
X	X	X	System-to-system (non-user) authentication tokens must not exceed a lifetime of 72 hours.
X	X	X	User-to-system authentication tokens must not exceed a lifetime of 10 hours.
X	X	X	User and non-user accounts must re-authenticate when requesting authorizations from a system with a higher assurance level than the requesting system.

Least Privileged Access Control

Least Privileged Access Control (CS-1557075)

Restrict access to all system components (i.e., application, operating system, and database) by performing the following:

Low	Med	High	Requirements
X	X	X	The assignment of access must be based on the principle of least privilege. Users must only be provided with the access essential to perform the tasks associated with their roles and responsibilities. Any access that is no longer required or needed must be removed.

Password Configuration

User Account Passwords (CS-10813512)

At a minimum, configure passwords for users as follows:

Low	Med	High	Requirements
X	X	X	Must be at least seven (7) characters in length.
X	X	X	Systems must require at least three (3) of the following parameters: Alpha characters (at least one) • Alpha characters (at least one) • Numeric characters (at least one) • Upper and lowercase characters (at least one) • Special characters • No repeating or sequential characters
X	X	X	Passwords must be protected against unauthorized access while at rest or in transit.
X	X	X	Password history must prevent users from reusing the same password within a minimum of four (4) rotations.
X	X	X	Must expire at least every 90 days.
X	X	X	Users must not be able to change their passwords more than once a day.
X	X	X	User accounts must be disabled after six (6) consecutive unsuccessful logon attempts. Access must be disabled for at least 30 minutes or until an administrator or another approved enterprise capability is used to unlock the account.

Non-User Account Passwords (CS-10813814)

At a minimum, configure passwords for non-users as follows:

Low	Med	High	Requirements
X	X	X	Must be at least fifteen (15) characters in length.
X	X	X	Systems must require at least three (3) of the following parameters: • Alpha characters (at least one) • Numeric characters (at least one) • Upper and lowercase characters (at least one) • Special characters • No repeating or sequential characters
X	X	X	Passwords must be protected against unauthorized access while at rest or in transit.
X	X	X	For interactive non-user accounts, after six (6) consecutive unsuccessful logon attempts, the account must prevent logon for at least 30 minutes or until an administrator unlocks the account.
X	X	X	If a non-user account is reactivated, the password must be changed upon first use.
X	X	X	Passwords for non-user accounts must be reset based on exposure or compromise.
X	X	X	Interactive non-user accounts must be managed by an approved enterprise password management tool. Effective Date Information: Non-User Account requirement effective Feb 1 2021 for all in-scope Compliance systems; effective Nov 1 2021, for all other systems.
X	X	X	Passwords for non-interactive non-user accounts must be stored in an approved enterprise secrets management tool. Effective Date Information: Non-User Account requirement effective Feb 1 2021 for all in-scope Compliance systems; effective Nov 1 2021, for all other systems.
	X	X	For PCI, SOX, GLBA and HIPAA systems only: The passwords for non-interactive non-user accounts must be changed annually.

Personal Identification Number (CS-16808341)

Configure Personal Identification Numbers (PINs) used as the sole authenticator to an IT Systems as follows:

Low	Med	High	Requirements
X	X	X	Must be at least six (6) digits long.
X	X	X	User accounts must be disabled after six (6) consecutive unsuccessful logon attempts. Access must be disabled for at least 30 minutes or until an administrator unlocks the account.
X	X	X	Systems must not allow repeating or sequential digits.
		X	Must expire at least every 90 days.
		X	PIN history must prevent users from reusing the same PIN within a minimum of four (4) rotations.

Access Provisioning and Removal

Access Provisioning (CS-1557076)

Require an approval to gain physical and logical access to information and facilities as follows:

Low	Med	High	Requirements
X	X	X	Access must be approved by either the user's manager, Access Owner or through an automated dynamic access ruleset prior to being granted.
X	X	X	For systems in scope for PCI, HIPAA, GLBA or SOX, systems with SHR data, or for privileged access: Access must be approved by the user's manager and Access Owner, or through an automated dynamic access ruleset prior to being granted.

Change in Role/Responsibilities (CS-35282090)

Protect Target assets when team members or third parties have a change in their roles or responsibilities.

Low	Med	High	Requirements
	X	X	For systems in scope for PCI, HIPAA, GLBA or SOX, systems with SHR data, or for privileged access: An individual’s access must be reviewed within 45 days of a change in job responsibilities. Access removals or modifications must be processed within 30 days of the access review.

Terminations (CS-35282417)

Protect Target assets when team members or third parties are terminated.

Low	Med	High	Requirements
X	X	X	Access must be disabled/revoked upon termination. The user account must be removed no later than 90 days after the termination date.

Inactive Account Reviews (CS-1557078)

Ensure user and non-user accounts are reviewed for inactivity.

Low	Med	High	Requirements
X	X	X	User accounts determined to be inactive for more than 90 days must be disabled or removed.
X	X	X	Non-user accounts must be deactivated or removed when the associated application or system is no longer needed.

Access Reviews (CS-1557079)

Perform access reviews of information systems and flag inappropriate access for removal as follows:

Low	Med	High	Requirements
X	X	X	For systems in scope for PCI, HIPAA, GLBA or SOX, systems with SHR data, or for privileged access: Access reviews of user and non-user production accounts, must be performed on a quarterly basis.
	X	X	Access must be revoked within 30 days following the quarter in which the user's access was identified for removal.

Access Control Rules Review (CS-1557080)

Ensure access rules are reviewed.

Low	Med	High	Requirements
X	X	X	Information system owners must perform an annual review of dynamic access rulesets and multi-entitlement roles.

Information System Owner Responsibilities

Information System Owner Responsibilities (CS-1557068)

Identify owners for information systems. Owner responsibilities include, but are not limited to, the following:

Low	Med	High	Requirements
X	X	X	The Information System Owner must maintain up to date Identity and Access control documentation and procedures for their system. At a minimum, the documentation must include: • An overview of the security model for the system/application • The definition of, use and assignment of privilege access • All available entitlements, their functions and assignment to user and non-user accounts
X	X	X	The Information System Owner must determine the access model for their Information System based on the principle of least privileged.
X	X	X	The Information System Owner is responsible for designing system access to prevent inappropriate access within or across systems.
X	X	X	The Information System Owner is responsible for accurately maintaining the relevant information needed to determine the security risk rating for their assigned Information System, maintaining an accurate asset inventory of the information system components, prioritizing and addressing security risks as needed and ensuring that the system complies with the relevant requirements defined within this policy document.
X	X	X	The Information System Owner is responsible for decommissioning their application if it is no longer needed.

Secure Delivery

Scope: Overall planning and process to ensure the secure development and delivery of information systems.

Product Planning

Product Team Security Responsibilities (CS-1557093)

All product team members are responsible for meeting information security requirements throughout the product lifecycle.

Low	Med	High	Requirements
X	X	X	The product teams must ensure that the selected infrastructure is approved for the workload based on the IT systems security risk rating, data classification and/or regulatory designation.
X	X	X	Engage Information Security when building or acquiring new applications or products: • contact the BISO, or • email security@target.com, or • post a query in the #security-help Slack channel Engage the Privacy Team at privacy@target.com if using guest or team member Personal Information (PI).

Secure Development Training (CS-1557094)

Ensure personnel have current secure coding training to protect against common coding vulnerabilities.

Low	Med	High	Requirements
X	X	X	Personnel involved with the development, integration, and/or delivery of IT assets must demonstrate an understanding of and apply common secure coding guidelines such as those described in the OWASP Top 10 Project or provided by Information Security via training and awareness activities.
		X	For systems in scope for PCI: Personnel must complete additional training upon hire and annually as required by PCI DSS.

Product Development

Delivery Model (CS-1557091)

Follow Target's approved product delivery methodology for products developed internally.

Low	Med	High	Requirements
X	X	X	Product changes must follow an approved change management process and meet the requirements defined within this policy document.

Product Security (CS-1557092)

Ensure all applicable information security requirements are integrated into product backlogs.

Low	Med	High	Requirements
X	X	X	The information security requirements must be actively managed as part of the product's backlog.
X	X	X	All requirements must include acceptance criteria.
X	X	X	Information security requirements that will not be met prior to production must be reviewed and approved by the Product Owner and Cybersecurity stakeholders (e.g., BISO, Compliance).

Product Documentation (CS-1557096)

Product documentation must be created and maintained.

Low	Med	High	Requirements
X	X	X	Product teams must maintain technical and product documentation, collect the appropriate information and maintain the necessary tools needed to support their IT systems.

Secure Coding

Component and Code Validation (CS-1557097)

Ensure software components (e.g., libraries, applications) and source code are secure prior to use.

Low	Med	High	Requirements
X	X	X	Third-party software components, packages, and integrations must be obtained from trusted sources.
X	X	X	Open source software components must be scanned for known vulnerabilities. Critical vulnerabilities must be remediated within 30 days of discovery. High risk vulnerabilities must be remediated within 90 days of discovery.
X	X	X	Workloads deployed into Target's environments must be sourced from an approved repository.

Protection of Application Code (CS-1557101)

Protect application code from unauthorized access.

Low	Med	High	Requirements
X	X	X	Source code must be stored in an approved version-controlled system and appropriately protected.
X	X	X	Access to binaries, libraries and load modules must be appropriately protected.

Secure Code Handling (CS-1557102)

Ensure source code and binaries are handled securely.

Low	Med	High	Requirements
X	X	X	Secrets (e.g., credentials, keys, access tokens) must be stored and accessed only in an authorized, secure manner.
X	X	X	Only Target-approved tools must be used to store and deploy code.

Security Testing

Pre-Deployment Validation (CS-1557098)

Ensure products undergo security due diligence prior to deployment into Target's environments.

Low	Med	High	Requirements
X	X	X	Functional and non-functional requirements, including the acceptance criteria must be documented.
X	X	X	The definition of done must be defined and documented.
X	X	X	Sensitive details and content, including PI and SHR data must be removed or obfuscated from production data before it is used in non-production environments.
X	X	X	All test data must be removed from the system prior to promotion to production.
		X	The penetration test team must be engaged prior to the initial production implementation.

Source Code Reviews (CS-1557100)

Ensure source code is reviewed for security vulnerabilities.

Low	Med	High	Requirements
X	X	X	All code changes to production IT systems must undergo an independent manual or automated code reviews to identify security defects. All security defects must be reviewed, validated and addressed as part of the development lifecycle.

Static Application Security Testing (CS-10810072)

Ensure application code is tested statically for security defects.

Low	Med	High	Requirements
X	X	X	All Target applications that are under active development are required to enroll for Static Application Security Testing scans.
X	X	X	All vulnerabilities discovered through the static scanning process must be reviewed, validated and addressed as part of the development lifecycle.

Dynamic Application Security Testing (CS-10810667)

Ensure security defects found during dynamic application security testing are handled appropriately.

Low	Med	High	Requirements
		X	All high risk applications that are externally accessible and internally developed are required to enroll for the ongoing Dynamic Application Security Testing scans. Vendor applications are excluded from this requirement.
		X	High severity application vulnerabilities must be reviewed, validated and where appropriate, remediated within 90 days of discovery.
		X	Medium severity application vulnerabilities must be reviewed, validated and where appropriate, remediated within 6 months of discovery.

Product Delivery

Application Programming Interface (API) Gateway (CS-10810910)

Ensure internal and external facing application programming interfaces (APIs) are appropriately maintained and exposed using the API Gateway.

Low	Med	High	Requirements
X	X	X	APIs that are consumed from outside of a product must be cataloged in a corporate registry and the catalog record must be kept up to date.
X	X	X	All externally accessible APIs must leverage the API Gateway.
X	X	X	API's must conform to the enterprise approved API Design Standard.
X	X	X	APIs must be appropriately secured.

Restriction of Access to Implement Changes (CS-1557105)

Restrict access to implementation changes.

Low	Med	High	Requirements
	X	X	For systems in scope for SOX, GLBA and HIPAA: Production environments, including hosts, databases, and applications must be safeguarded against or monitored for unintentional and unauthorized changes.
	X	X	For systems in scope for SOX, GLBA and HIPAA: Segregation of duties must be enforced to ensure that the person conducting the review and approval of the file modifications is not the same person whose activities are being monitored.
X	X	X	Production environments must be restricted and segregated from the development environments.

Product Operations

System Vulnerability Testing (CS-1557148)

Ensure production systems are tested to identify weaknesses or security vulnerabilities.

Low	Med	High	Requirements
		X	For systems in-scope for PCI: Penetration tests must be performed by approved personnel at least annually or upon a significant change in the system or system environment.
		X	For internally developed Internet-facing or publicly accessible applications and APIs, perform ongoing Dynamic Application Security Testing scans.
		X	Non-PCI applications must be assessed by the penetration team at least every two years or upon a significant change in the application, network or environment.

Platform Vulnerabilities (CS-35290285)

Ensure production platforms are tested to identify weaknesses or security vulnerabilities.

Low	Med	High	Requirements
X	X	X	Vulnerability scans must be performed at least quarterly and after a significant change in the network or environment.
X	X	X	Critical vulnerabilities must be remediated within 30 days of discovery. High risk vulnerabilities must be remediated within 90 days of discovery.
X	X	X	Critical and high risk vulnerabilities must be rescanned to confirm successful remediation.
X	X	X	Active vulnerabilities must be prioritized for remediation.
X	X	X	Monitor industry sources for information about technical vulnerabilities that affect Target.
		X	For systems in scope for PCI: Vulnerability scans must be performed by approved personnel.

IT Operations

Scope: Overall planning and processes to enable secure and continuous IT services through effective operational procedures.

Security During Operations Changes

Systems Maintenance (CS-1557111)

Ensure IT systems are maintained to prevent degradation.

Low	Med	High	Requirements
X	X	X	Systems must be on a currently supported version for which security patches continue to be provided.
X	X	X	Document maintenance procedures for systems that include, as applicable: patch management, upgrades, business strategies, required security reviews and requirements.
X	X	X	Review and approve maintenance procedures annually.

Patch Management (CS-1557112)

Ensure systems and applications stay updated by installing vendor patches.

Low	Med	High	Requirements
X	X	X	Industry/vendor sources must be monitored for alerts and notifications of new configuration changes, patches, hot fixes, upgrades and new service packs.
X	X	X	Critical security patches and vendor recommended configuration changes must be installed or implemented within 30 days of release. All other security patches and changes must be installed or implemented within 90 days of release.

Change Management (CS-1557113)

Track changes to IT systems, including software, hardware, and network, through approved central change management systems.

Low	Med	High	Requirements
X	X	X	Changes to production IT systems, must follow an approved change management process.
X	X	X	The impact of changes must be reviewed and communicated to the relevant stakeholders.
X	X	X	Changes must be planned and managed to minimize conflicts and interruptions.
		X	Risk mitigation strategies must be determined for high risk changes.
X	X	X	The change management procedures, including change approvers must be documented.
X	X	X	The change approval must be documented.
	X	X	For systems in scope for SOX, GLBA, and HIPAA: The responsibility to approve and implement changes must be segregated and appropriately restricted, unless the production environment is monitored for unintentional and unauthorized changes.
	X	X	For systems in scope for PCI, SOX, GLBA, and HIPAA: Changes to production IT systems must only be approved, after verifying that the requirements specified within this policy document have been satisfied.
X	X	X	All changes to production IT systems must be recorded.
X	X	X	Backout plans must be documented.
X	X	X	Changes to production IT systems must be tested.
	X	X	For systems in scope for PCI, SOX, GLBA, HIPAA: The test procedures and test results must be documented.

Review Production Changes on Regular Basis (CS-1557115)

Production changes are reviewed by management.

Low	Med	High	Requirements
	X	X	For SOX systems and high risk rated systems, management generates a system report of production changes and reviews the changes on a regular basis to ascertain that they are appropriate and approved by management.

Automation Requirements (CS-1557116)

Implement automated tools to support efficiency and reduce errors.

Low	Med	High	Requirements
X	X	X	Implement automated tools to accomplish daily operational tasks as determined by enterprise IT management.

Managing New System Releases from Vendors (CS-1557117)

Require vendors to provide advance notice of system releases and review changes for impact.

Low	Med	High	Requirements
X	X	X	For systems in which a vendor is responsible for managing and installing system releases and updates, require advance notification of new releases and updates.
X	X	X	Analyze changes for business or administrative impacts.
X	X	X	Coordinate release and deployment activities, and track changes.

Project Training Requirements (CS-1557118)

Ensure users are trained on new systems and upgrades.

Low	Med	High	Requirements
X	X	X	Identify training requirements when deploying major hardware or software systems or upgrades to minimize the impact on administrators and end users.

Monitoring and Resolving Processing Errors (CS-1557119)

Ensure systems are monitored for processing errors.

Low	Med	High	Requirements
	X	X	For systems in scope for SOX: Critical systems, programs, and/or jobs are monitored, and processing errors are corrected to ensure successful completion.

Product Decommissioning (CS-10811089)

Ensure products and their associated environments are decommissioned securely.

Low	Med	High	Requirements
X	X	X	Data and media must be disposed in accordance with Target's Records and Information Management Policy and Records Retention Schedules as well as secure disposal of media procedures.

Secure Hardening and Configuration Management

Configuration Management Procedures (CS-1557120)

Ensure configuration management and baseline practices are followed.

Low	Med	High	Requirements
X	X	X	Create, document, and adhere to configuration baselines that implement Target's security policies.
X	X	X	Store configuration baselines and implementations in approved central repositories.
X	X	X	Review configuration baselines annually or upon significant change to the technology (e.g., new/altered security parameters, OS update or upgrade, new policy requirements).
		X	For systems in scope for PCI: Only one (1) primary function is allowed to be implemented per server.
		X	For systems in scope for PCI: Additional security features must be implemented to address the security risks that are created by using required services, protocols or daemons that are considered to be insecure or do not meet Target's security requirements.

Vendor Defaults (CS-1557121)

Change vendor defaults for security related secrets for all systems, including but not limited to: wireless systems, devices, software, security services, application and system accounts, and Point of Sale (POS) terminals.

Low	Med	High	Requirements
X	X	X	Change all default secrets in systems (e.g., passwords, encryption keys, certificates, SNMP community strings).
X	X	X	Unnecessary software, services and accounts must be removed or disabled.

Configuration Scanning (CS-1557122)

Ensure configuration management and baseline practices are validated.

Low	Med	High	Requirements
	X	X	For systems in scope for PCI, HIPAA, GLBA, SOX, or systems with SHR data: Servers and databases must be scanned against a configuration baseline on a semi-annual basis (twice a year). Scan results that indicate a divergence from the baseline must be addressed in accordance with the Security Finding Process for remediation.

Preventing Installation of Unauthorized Software (CS-1557123)

Ensure only approved software is installed on systems.

Low	Med	High	Requirements
X	X	X	Controls must be implemented to prevent or detect the installation of unauthorized software on systems.

System Clocks (CS-1557124)

Ensure system clocks are accurately synchronized.

Low	Med	High	Requirements
X	X	X	Keep system clocks current by synchronizing to an approved time source.
		X	For systems in scope for PCI: Time data must be protected and only received from an industry-accepted time source.

User Login Requirements (CS-1557125)

Ensure login prompts are configured securely.

Low	Med	High	Requirements
X	X	X	The specific system or application version information must not be displayed until the user has successfully authenticated.
X	X	X	The system or application must not display which part of the credential was incorrectly entered after a failed log-on attempt.
X	X	X	The password being entered must never be displayed.
X	X	X	User sessions must be unique per user and computationally very difficult to predict.
	X	X	Systems must display a notice indicating that only authorized use is permitted on Target's Information Systems.

Modifications to Software Packages (CS-1557126)

Limit modifications to software packages.

Low	Med	High	Requirements
X	X	X	Limit modifications to software packages such that changes do not affect vendor support of the software.

Data Sharing Between Systems (CS-1557127)

Protect the confidentiality, integrity, and availability of data shared between systems.

Low	Med	High	Requirements
X	X	X	Information must only be shared between systems when required for business purposes.
X	X	X	Product teams must ensure that their IT systems meet the security requirements for the classification of data consumed by their IT systems.

Imaging Systems Configuration (CS-1557128)

Ensure compatibility with imaging systems.

Low	Med	High	Requirements
X	X	X	Configure imaging hardware and software to be interchangeable with that of other vendors.

Information Technology Help Desk (CS-1557129)

Implement an IT help desk function to support the organization.

Low	Med	High	Requirements
X	X	X	Create a working knowledge base of common issues.
X	X	X	Create a process to prioritize recorded help desk issues.

Network Security

Scope: Overall security and risk management framework to protect the confidentiality and integrity of IT infrastructure and network assets.

Network Access Control

Internal and External Network Access (CS-1557130)

Ensure user access to networks and network services does not compromise the security of the network.

Low	Med	High	Requirements
X	X	X	Authenticate devices that connect to the internal network from an external network.
X	X	X	Remote access to the internal network must utilize strong authentication and be protected using a secured tunnel.

Inbound and Outbound traffic on Networks (CS-1557131)

Implement controls over inbound and outbound traffic.

Low	Med	High	Requirements
X	X	X	All inbound and outbound traffic between network zones must be denied unless explicitly allowed.
X	X	X	Private IP address and routing information must not be disclosed to the internet.
X	X	X	RFC1918 traffic originating from the Internet must be blocked.
X	X	X	All outbound traffic to the internet must pass through a broker device (e.g., firewall or proxy).
X	X	X	All inbound traffic must pass through an IDS or IPS.
X	X	X	Inbound and outbound traffic must be inspected based on risk.
X	X	X	Only authorized traffic is permitted to be disclosed to authorized external parties.
X	X	X	Only authenticated devices must be allowed to connect to the internal network from an external network.
X	X	X	User traffic must be authenticated.

Monitor Network Traffic (CS-1557163)

Monitor network traffic for suspected compromises.

Low	Med	High	Requirements
X	X	X	Intrusion detection or prevention systems must be used to monitor network traffic and alert personnel to anomalies.
X	X	X	Intrusion-detection and prevention engines, and signatures must be kept up-to-date.
		X	For systems in scope for PCI: Intrusion-detection systems and/or intrusion-prevention systems must be used to monitor traffic at the perimeter of the cardholder data environment, as well as at critical points inside the cardholder data environment to alert personnel of suspected compromises.

Third-Party Network Connections (CS-1557132)

Ensure the security of third-party network connections.

Low	Med	High	Requirements
X	X	X	External third-party network connection requests, including the business justification and use case must be documented, reviewed and approved prior to the connection being configured or setup.

Network Device Management

Network Documentation (CS-1557133)

Maintain network documentation.

Low	Med	High	Requirements
X	X	X	The network documentation must maintained and updated on at least an annual basis or subsequent to a significant change in the network environment.
X	X	X	The network services, protocols and ports used between network zones along with the business justification for each must be documented.

Firewall Configuration Standard (CS-1557134)

Implement firewall controls to block unwanted and malicious traffic.

Low	Med	High	Requirements
X	X	X	Only authorized traffic must be allowed between the Internet, Demilitarized Zones (DMZs), internal networks, production environments, non-production environments, extranets, third-party connections, and secure segments.
X	X	X	Firewalls must be configured to fail closed in the event of a failure.
X	X	X	All inbound and outbound traffic must be denied unless explicitly allowed.
X	X	X	Firewall and router rule sets must be reviewed at least annually.
		X	For systems in scope for PCI: Firewall and router rule sets must be reviewed every six months.
		X	For systems in scope for PCI: Perimeter firewalls must be installed between any wireless network and the payment card environment.
		X	For systems in scope for PCI: Permit only authenticated connections into the network.
		X	For systems in scope for PCI: The perimeter firewalls must be configured to deny all traffic from the wireless network unless the network traffic is specifically allowed due to its necessity for business purposes.
		X	For systems in scope for PCI: Network traffic that is specifically allowed due to its necessity for business purposes must be controlled by the perimeter firewalls.

Router and Firewall Start-up Files (CS-1557135)

Ensure router and firewall configuration files are secured and synchronized.

Low	Med	High	Requirements
X	X	X	The default firewall and/or router configuration files must be configured to deny all connections unless explicitly authorized.
X	X	X	The firewall and/or router configuration files must maintained and kept up to date as appropriate.
X	X	X	The firewall and/or router configuration files must be protected against unauthorized access and/or change.

Web Application Firewalls (CS-1557136)

Ensure web application traffic is inspected for malicious payloads.

Low	Med	High	Requirements
		X	HTTP / HTTPS traffic to internet facing systems or services must be inspected by a web application firewall.

Personal Firewall Software on Mobile and Employee-Owned Computers (CS-1557137)

Ensure firewall software is installed on required devices.

Low	Med	High	Requirements
		X	For systems in scope for PCI: Personal firewall software or software with the equivalent functionality must be installed on any internet connected mobile or employee owned laptop computer used to access cardholder data.

Authorize Wireless Access Points (CS-1557138)

Ensure only authorized wireless access points are connected to Target networks.

Low	Med	High	Requirements
		X	For systems in-scope for PCI: Scans to detect unauthorized/rogue wireless access points connected to Target's network must be performed at least quarterly.
		X	For systems in-scope for PCI: All detected unauthorized/rogue wireless access points must be reported and addressed in accordance to Target's incident response procedures.
X	X	X	An inventory of authorized wireless access points, including the documented business justification for each access points or groups of access points must be maintained.
X	X	X	The guest wireless network must be logically separated from the internal wireless network.

Wireless Device Encryption (CS-1557139)

Configure wireless devices (e.g., access points, wireless clients) to use strong encryption.

Low	Med	High	Requirements
X	X	X	Wireless access devices must use strong encryption technology for authentication and transmission.

Domain Name System (CS-1557140)

Ensure the security of Domain Name Systems.

Low	Med	High	Requirements
X	X	X	DNS servers with internal roles must only process name and address information resolution requests from within Target.
X	X	X	DNS servers with external roles must only process name and address information resolution requests from clients external to Target.
X	X	X	At least two internal and one external authoritative DNS servers must be deployed.
X	X	X	DNS servers must be deployed in at least two separate physical locations.

Access to Diagnostic and Configuration Ports (CS-1557141)

Ensure access to diagnostic and configuration ports is secured.

Low	Med	High	Requirements
X	X	X	Physical access to diagnostic and configuration ports must be appropriately restricted.
X	X	X	Remote access to diagnostic and configuration ports must occur over a secured channel and adhere to authentication requirements (CS-1557069).
X	X	X	Logical access to diagnostic and configuration ports must be secured in accordance with the requirements defined in control CS-1557069.
		X	For systems in scope for PCI: Privileged access to IT systems located within the Cardholder Data Environment must utilize multi-factor authentication.

Network Segmentation

Network Zoning (CS-1557142)

Ensure systems are securely segmented.

Low	Med	High	Requirements
X	X	X	Services, users and/or systems must be segregated into logical network zones or segments based on the sensitivity of information.
		X	For systems in scope for PCI: System components that store cardholder data must be placed in an internal network zone that is segregated from the DMZ and other untrusted and non-PCI systems.

DMZ Configuration (CS-1557143)

Implement firewall DMZ configuration controls to filter and screen inbound and outbound Internet traffic.

Low	Med	High	Requirements
X	X	X	Inbound traffic associated with systems that are internet facing or publicly accessible must terminate at the DMZ.
		X	For systems in scope for PCI: Outbound traffic from payment card applications must be restricted to IP addresses that are inside the DMZ.
		X	For systems in scope for PCI: Any inbound or outbound direct routes for traffic between the Internet and the cardholder environment is not allowed.

Shared Hosting Provider Requirements (CS-1557144)

Ensure cardholder data is protected when acting as a shared hosting provider.

Low	Med	High	Requirements
		X	For systems in scope for PCI: Shared hosting providers must restricted all the processes, access and privileges of an entity to its own secure segment data environment.
		X	For systems in scope for PCI: Shared hosting providers must enable logging for each secure segment data environment and enable processes for timely forensic investigations in the event of a compromise.

Enterprise Network Solutions

Public Network eCommerce (CS-1557145)

Ensure electronic commerce information (e.g., online transactions, payments) is protected.

Low	Med	High	Requirements
	X	X	Product teams must utilize protocols that support the accuracy and integrity of business critical transactions.

Threat and Incident Management

Scope: Overall approach to perform security through risk and threat mitigation.

Security Logging and Analytics

System Activity Logging (CS-1557150)

Log system activities to be able to reconstruct the following events (also see CS-1557151 for details):

Low	Med	High	Requirements
	X	X	For systems in scope for PCI, HIPAA, GLBA, SOX or high risk systems: The following events must be logged if they are performed by the Information System: **Authentication and Authorization** • Success (should contain source and user information) • Failure (should contain source, user information, and failure reason) **Process Execution** • Process start (should contain process arguments) **Privilege and Permission Changes** • Changes to local user accounts • Changes to local groups • Ownership changes • Permission changes **System Configuration Changes** • Security configuration changes • Configuration file changes • Service changes (start, stop, enable, disable, modify) • File system changes **SHR Data Access** • User read access • User modifications to data **Business Critical Data Access** • User modifications to data
X	X		The following operating system events must be logged: **Process Execution** • Process start (should contain process arguments)
		X	Read access attempts to SHR data stored on disk must be logged.

Log Capture (CS-1557151)

Ensure that sufficient detail about the activity is captured in the logs to recreate events.

Low	Med	High	Requirements
X	X	X	For each event logged (per CS-1557150), the following details must be captured to facilitate event re-creation: • User identification • Type of event • Date and timestamp in UTC or ISO-8601 compliant format • Success or failure indication • System performing the event
X	X	X	The System Owner must review and where appropriate, update the data types and logging configuration settings at least annually.
		X	System logs must not capture Secure Handling Required (SHR) data.
	X	X	Access to system logs must be restricted based on the principle of least privilege.

Retain and Protect Activity Logs (CS-1557152)

Ensure system activity logs are available, accessible, and accurate.

Low	Med	High	Requirements
X	X	X	System activity logs must be physically and logically protected from modification and/or deletion.
X	X	X	The ability to de-activate system activity logging must be restricted or monitored.
X	X	X	At a minimum, log data must be retained for up to one week unless being streamed to a logging pipeline.
	X	X	For systems in scope for PCI, HIPAA, GLBA, SOX: Product teams must stream their log data to a logging pipeline.
	X	X	For systems in scope for PCI, HIPAA, GLBA or SOX: The log data for the past 400 days must be retained.
		X	For systems in scope for PCI: The log data for the past three months (90 days) must immediately be available online.

System Monitoring (CS-1557153)

Ensure systems are monitored to detect malicious or unwanted activity.

Low	Med	High	Requirements
	X	X	Employ segregation of duties to ensure the person conducting the log review is not the person whose activities are being monitored.
	X	X	Product teams must periodically inspect their IT system logs for malicious or unwanted activity based on risk; Software automation can be used to detect and subsequently alert on malicious or unwanted activity; All detected malicious or unwanted activity must be addressed and reported to appropriate personnel.
		X	For systems in scope for PCI Critical log data must be inspected for known malicious activities.
		X	For systems in scope for PCI: Non-critical logs must be reviewed based on the results of periodic risk assessments.

Threat Management

Protect Against Malicious Software (CS-1557154)

Protect Target’s environment from malicious software.

Low	Med	High	Requirements
X	X	X	IT systems commonly affected by malware must be protected by anti-virus programs, capable of detecting, removing and protecting against malicious software.
X	X	X	Anti-virus programs must be current, actively running and generating audit logs. Users must not be able to disable or alter these programs.
		X	For systems in scope for PCI: The Information System Owners, must perform an annual evaluation of the systems that are not commonly affected by malicious software and determine whether such systems require anti-virus software.

Change Detection Tools (CS-1557155)

Implement Change Detection tools to monitor files and applications as follows:

Low	Med	High	Requirements
		X	For systems in scope for PCI: Critical system, application, configuration and content files, must be monitored for unintentional and unauthorized changes.
		X	For systems in scope for PCI: File modification alerts, must be reviewed, investigated and resolved in a timely manner.

Incident Management

Incident Response (CS-7027487)

Enable visibility to system endpoints to permit endpoint inventory and quick detection of vulnerabilities that may require incident response.

Low	Med	High	Requirements
X	X	X	Enterprise inventory and incident response tools (e.g., Tanium) must be current and actively running.

Third-Party Security

Scope: Overall processes, procedures, and enabling technology to identify and manage information security risks in doing business with third parties. The Third Party Security Policy is built in relation to Target's Vendor Risk Management Policy. Refer to the Vendor Risk Management Policy for additional vendor management requirements, i.e., engagement, management and/or termination.

Third-Party Due Diligence

Third-Party Due Diligence (CS-1557106)

Perform a due diligence review prior to executing a contract with a third party.

Low	Med	High	Requirements
X	X	X	The Target RM is responsible for ensuring that the third-party is financially viable and that its services and/or product(s) meet Target's technical specifications, business continuity expectations, and functional/operational requirements.
X	X	X	For third-parties that will have access to Target's SHR or Confidential information or that will connect to Target's information systems or network: The Target RM is responsible for ensuring that a third-party security assessment is complete prior to sharing SHR or confidential data with the third party or connecting the vendor to Target's information systems or network.
X	X	X	The Target RM is responsible for ensuring that the third-party security findings are addressed before giving the third-party access to Target's SHR or Confidential information or giving them access to the Target's information systems or network.

Contract Management

Contracting with Third Parties (CS-1557107)

Ensure security considerations are built into contract agreements with third parties by performing the following:

Low	Med	High	Requirements
	X	X	The Target RM must establish an Information Security Agreement/Addendum (ISA) with third parties that will (a) handle personally identifiable information (PII) about Target team members or guests; or (b) connect to a Target's information system or network; or (c) handle highly sensitive business information prior to engaging services with the third party.
		X	For GLBA systems only, include escrow rights in contracts, as applicable. Require software vendors to inform Target if the software vendor pledges the software as loan collateral.

Software Licenses and Warranties (CS-1557108)

Ensure security considerations are built into software licenses and warranties as follows:

Low	Med	High	Requirements
X	X	X	The Target RM is responsible for ensuring that the approved contract terms include software licenses and warranties and are reviewed by the designated approvers.

Termination of Third Parties (CS-1557109)

Ensure third-party termination processes are followed upon completion of a contract by performing the following:

Low	Med	High	Requirements
X	X	X	The Target RM is responsible for meeting all the requirements in the Vendor Risk Management Policy.
X	X	X	The Target RM must collect or confirm the destruction of Target's Information and/or assets from the third party.

Ongoing Third-Party Risk Review and Monitoring

Ongoing Third-Party Risk Review and Monitoring (CS-1557110)

Ensure third parties are meeting security requirements by performing the following:

Low	Med	High	Requirements
X	X	X	The Target RM is responsible for ensuring that the vendor meets their security obligations and appropriately address the gaps in their security controls or initiate plans to terminate the vendor relationship.
		X	Target RMs must support Target's ongoing security evaluation, regulatory or compliance (e.g. PCI) reviews and event response involving their third party(s).

Physical and Environmental Security

Scope: Overall management of physical security including controls for Target-operated facilities, equipment, and third party IT facilities.

The Physical and Environment Security Policy is built in relation to the Visitor Management Policy (US Only) to ensure the safe and secure environment at Target locations (Headquarters, Stores and Distribution Centers). Please reference the Visitor Management Policy (US Only) for more details and requirements.

Secure Areas

Physically Secure IT Facilities, HQ Facilities, and Sensitive Areas (CS-1557081)

Physically secure IT facilities processing Target data, HQ facilities, and other sensitive areas to prevent unauthorized individuals from gaining access.

Low	Med	High	Requirements
X	X	X	Access points must be properly controlled using security perimeters to prevent unauthorized access.
X	X	X	Access must be restricted based on the principles of least privilege. Visitors must be escorted when in sensitive areas.
		X	For systems in scope for PCI: Network access points that could be a pathway to cardholder data must be appropriate restricted.

Physically Securing Sensitive Data (CS-1557082)

Physically secure sensitive data to protect the data from unauthorized access.

Low	Med	High	Requirements
	X	X	Physical access to Confidential and SHR data must be restricted by placing such information in locked facilities, storage areas, or containers.
		X	For systems in scope for PCI: Devices used for transactions or the processing of cardholder data must be physically secured.
		X	For systems in scope for PCI: Card-reading devices must be periodically inspected to detect tampering or a substitution of the device.

Badge Identification for IT and HQ Facilities (CS-1557083)

Require that individuals (employees, contractors, and third parties) are identifiable at IT and HQ facilities.

Low	Med	High	Requirements
X	X	X	Each individual must be issued with a unique ID badge.
X	X	X	Individuals must display their badge for identify verification purposes.

Manage Visitor Access for IT and HQ Facilities (CS-1557084)

Secure IT and HQ facilities by managing the physical access for visitors.

Low	Med	High	Requirements
X	X	X	Visitors must be issued with badges or access devices that expires and identifies them as non-employees.

Physical Surveillance Monitoring (CS-1557085)

Perform physical access monitoring on IT Facilities, HQ Facilities, and other sensitive areas to prevent and detect unauthorized access.

Low	Med	High	Requirements
X	X	X	Physical access to HQ facilities, data centers and other locations with sensitive information or systems must be monitored.
X	X	X	Monitoring devices (e.g. video cameras) must be protected from tampering.
	X	X	Information (e.g., video tape, badge access logs) must be retained in accordance to the Records and Information Management program’s Records Retention Schedule.
		X	For systems in scope for PCI: Facilities that process or store cardholder data must review the collected monitoring data, including correlating the data with other data sources to identify potential access issues.

Data Center Physical Access Review (CS-1557086)

Monitor physical access to data centers to ensure access is granted only to authorized individuals.

Low	Med	High	Requirements
X	X	X	Data center access reviews must be performed on a quarterly basis.

Guest Payment Devices (CS-1557087)

Protect guest payment devices (e.g., credit card readers).

Low	Med	High	Requirements
		X	For systems in scope for PCI: Guest payment devices must be periodically inspected to detect tampering.
		X	For systems in scope for PCI: An up-to-date inventory of guest payment devices must be maintained.
		X	For systems in scope for PCI: Personnel must be trained to be aware of attempted tampering or replacement of guest payment devices.
		X	For systems in scope for PCI: The make and model of the devices used to capture the payment card data through physical interaction must be recorded and maintained.

Safeguards and Maintenance

Environmental Safeguards (CS-1557088)

Implement environmental safeguards to protect information-processing facilities.

Low	Med	High	Requirements
X	X	X	Information-processing facilities must be protected from extreme temperatures, fire, water or other environmental hazards.
X	X	X	Heat/smoke detectors and fire resistance barriers (e.g. doors, walls) must be installed to protect equipment from fire damage.
X	X	X	Water detectors and floor drains under raised floors must be installed to prevent possible water damage.

Power and Telecommunications Cabling Security (CS-1557089)

Secure power and telecommunication cabling against threats.

Low	Med	High	Requirements
X	X	X	All above-ground power and telecommunication cabling must be separated from each other and the appropriate security measures must be taken to prevent physical damage and data or signal interception or interference.
X	X	X	Equipment must be protected from power failures or other disruptions.

Information Processing Facilities Preventive Maintenance (CS-1557090)

Perform preventive maintenance on physical security assets at information-processing facilities to ensure they remain functional.

Low	Med	High	Requirements
X	X	X	Physical security related components must undergo preventative maintenance in accordance with a pre-determined schedule.
X	X	X	Records of repairs and modifications must be retained.
X	X	X	Maintenance must only be performed by authorized organizations or personnel.

Disaster Recovery

Scope: Overall planning and processes to ensure the recovery and availability of critical information during a disaster. The Disaster Recovery Policy is built in relation to Target Continuity Policy. Please visit the Target Continuity Policy for a list of all business continuity management requirements.

Disaster Recovery

Disaster Recovery Plans (CS-1557156)

Implement disaster recovery plans in accordance with the following:

Low	Med	High	Requirements
	X	X	The Disaster Recovery team must document, maintain and communicate the roles, responsibilities and recoverability requirements of the disaster recovery program.
	X	X	The Information System Owner must identify and document the recovery procedures to undertake following an interruption to, or failure of their IT system.
	X	X	The Information System Owner must update the disaster recovery plan after any significant changes in the system or system environment.
	X	X	Disaster recovery plans must be formally approved by both the Disaster Recovery team and a Level 7+ Leader. Disaster recovery plans are not valid until they are approved by both the Disaster Recovery team and the Level 7+ Leader.

Disaster Recovery Plan Testing (CS-1557157)

Ensure that the Disaster Recovery plan is performing as it is designed.

Low	Med	High	Requirements
	X	X	The Information System Owner must validate the effectiveness of the recovery procedures by testing the recoverability of the IT system at least annually.
	X	X	New P1/P2 systems must complete a disaster recovery test within 90 days of going into production.
	X	X	The Information System Owner must update the disaster recovery plan based on the recovery test results.
	X	X	The Disaster Recovery team must formally accept the disaster recovery test.

System Documentation Protection (CS-1557158)

Ensure system documentation is secure with the following:

Low	Med	High	Requirements
	X	X	System related documentation, used to recovery of the system, must be protected from unauthorized access, modification, removal, and/or destruction.
	X	X	The data recovery procedures must be stored at a different location from the site of the computer equipment processing the data.

System Redundancy and Fault Tolerance (CS-1557159)

Ensure that critical systems are safeguarded from single points of failure.

Low	Med	High	Requirements
	X	X	Systems must be engineered and designed with adequate redundancy and/or fault tolerance.
	X	X	Systems must be engineered per disaster recovery principles and patterns.

Data Preservation and Continuity (CS-1557160)

Ensure continuity of technology operations by preserving data and enabling its recoverability within reasonable timeframes to support the business.

Low	Med	High	Requirements
X	X	X	The capability to recover data must meet business requirements. As applicable, data may be restored to a pre-defined recovery point objective.
X	X	X	Backups or refresh safe copies of data must be performed as needed to meet the recovery point objective of the IT system.
X	X	X	Data backups, replications or other data continuity processes must be monitored to ensure successful execution. Failures must be corrected as needed.
X	X	X	The Information System Owner must define the retention period, media type, frequency and location for backups, replications and other data continuity measures.
X	X	X	The Information System Owner must validate the effectiveness of the data preservation and continuity strategy, at least annually, to ensure that production data can be restored as expected.

Recovery Facility Security (CS-1557161)

Ensure recovery facilities protect critical assets at the same level of security, as the primary site.

Low	Med	High	Requirements
X	X	X	The recovery facility must meet the security requirements listed within this Information Security Policy.
X	X	X	The Information System Owner must consider potential accessibility problems in the event of an area-wide disruption or disaster, and outline mitigation actions as part of the site selection process.
X	X	X	Priority service agreements must be obtained with applicable service providers.

Emergency Access to Information (CS-1557162)

Ensure that critical job functions have access to critical information during an emergency.

Low	Med	High	Requirements
	X	X	Adequate procedures must be implemented to ensure that the necessary electronic information is accessible in the event of a disaster.

Human Resources Security

Scope: Overall management and controls to ensure security of contractor and team member resources from pre-employment/pre-engagement through termination.

Pre-Employment/Pre-Engagement

Candidate Pre-Employment/Pre-engagement Due-Diligence (CS-1557049)

Ensure due-diligence is performed for all candidates (i.e., team members and contractors) within 30 days of employment/engagement.

Low	Med	High	Requirements
X	X	X	Background verification checks must be completed for candidates in proportion to the job duties.
X	X	X	Candidates must sign the terms and conditions that include accepting any actions taken if they are found non-compliant with the requirements listed within the Information Security Policy.
X	X	X	Candidates must sign the applicable confidentiality agreements and/or non-disclosure agreements.

Employment/Engagement

Information Security Compliance (CS-1557050)

Ensure that team members and contractors secure Target assets during their employment or assignment.

Low	Med	High	Requirements
X	X	X	Individuals must comply with the information security requirements outlined in the Information Security Policies. Do not use Target assets to perform illegal or unethical activities.
X	X	X	Team members who violate Target's Information Security Policies may incur disciplinary action, up to and including immediate termination. Violators may also be subject to legal action, including criminal prosecution. Target reserves the right to take any other action it believes is appropriate.
X	X	X	Contractors who violate Target's Information Security Policies may have their assignment terminated. Violators may also be subject to legal action, including criminal prosecution. Target reserves the right to take any other action it believes is appropriate.
X	X	X	Report non-compliance to security@target.com. This includes if you are unable to comply with the Information Security Policies or you are aware of a situation that is a security risk. If you would like to remain anonymous, you may contact the Integrity Hotline at 1-800-541-6838 (individuals in U.S.); 000-800-100-1657 (individuals in India); 470-219-7116 (individuals in other non-U.S. locations); or report online at Integrity@Target.com.
X	X	X	Security findings must be remediated in accordance with the Information Security Finding Process.

Critical Roles and Job Functions (CS-1557051)

Limit the disruption of service to Target critical functions by ensuring redundancy in staff knowledge.

Low	Med	High	Requirements
X	X	X	Key roles and job functions must be supported through knowledge capture, knowledge sharing and staffing backups.

Asset Recovery upon Termination (CS-1557052)

Protect Target-issued assets as follows:

Low	Med	High	Requirements
X	X	X	Target-issued assets, including information, must be collected upon termination or at the end of an assignment.

Related Policies and Documents

- Application Asset Risk Rating
- Information Security Finding Process
- Information Security Training
- Privacy Compliance Policy
- Records and Information Management Policy
- Target Continuity Policy
- Vendor Risk Management Policy
- Visitor Management Policy (US Only)

Appendix A: Definitions

Definitions of the terms used in the Information Security Policy.

Access refers to the ability to obtain, examine, or retrieve view-protected information held by an organization.

Access Model is a system design approach that defines the controls that provide security to an application, system or platform.

Access Owner - *see Information Systems Owner.*

Access Provisioning and De-provisioning is the process of granting information technology systems access to authorized users and communicating the newly issued credentials to the user or user's manager. Access de-provisioning is the process of removing information technology systems access from users who are no longer authorized or no longer need the access.

Access Approval is the process by which an authorized person approves access to an IT system.

Active Vulnerabilities are vulnerabilities that present an immediate risk to Target, based on its high exploitation likelihood, catastrophic impact, or reputation damage, as determined by the Cyber Fusion Center and Endpoint Security's Active Vulnerability Management process.

Adaptive Authentication - *see Authentication.*

Affiliate refers to any company that controls, is controlled by, or is under common control with another company.

Application includes purchased and custom software programs or groups of programs, including both internal and external (e.g., web) applications.

Application Vulnerabilities are vulnerabilities caused by flaws in code, in settings or other issues that occur in the running application or overall business logic that impacts how the application operates or integrates with other applications.

Assurance Level, as it pertains to authentication, describes the level of confidence that the credentials presented by a user or entity actually belong to and identify that user or entity.

Authentication is the process of verifying the identity of an individual, device, or process prior to authorizing access to a system. Authentication typically occurs using one or more authentication factors, such as something you know, (e.g., a password); something you have, (e.g., a token device or smart card); something you are, (e.g., a biometric); something you do habitually (e.g. log directly into the Target network from the office using a Target-owned device).

- **Adaptive Authentication** refers to a matrix of variables whose combination results in a risk profile. Based on the risk profile, additional authentication requirements may be added before certain functions can be performed
- **Multi-Factor Authentication** refers to requiring the successful presentation of two or more authentication factors to gain access to a system
- **Strong Authentication** is a categorization of authentication protocol that requires more than just an account ID and password to gain access to a system. Two-factor authentication, multi-factor, and adaptive authentication are considered strong authentication
- **Two-Factor Authentication** is a subset of multi-factor authentication that requires the successful presentation of two factors

Authoritative Source is any applicable law, regulation, and industry standard that is in scope and drives information security requirements.

Authorization in the context of access control is the granting of access or other rights to a user, program, or process. Authorization defines what an individual or program can do after successful authentication.

Biometrics are unique identifiable data about an individual's body (e.g., fingerprint, eye scan, facial recognition, etc.).

Broker Device refers to a firewall or proxy server that acts as an intermediary between a workstation user and the Internet so that the organization can ensure security, administrative control, and caching service.

Business Critical Data is critical to business operations or regulatory compliance.

Business Critical Transactions refer to online transactions that are deemed to be critical to business operations or regulatory compliance.

Business Unit Management refers to the individual(s) who, based on policies and clearly defined objectives, oversee(s) the activities of a team.

Card Verification Security Code is a three- or four-digit security verification code or value printed or embossed on a credit/debit card. The following list provides the security code terms used by each card brand:

- CID - Card Identification Number (American Express and Discover payment cards)
- CAV2 - Card Authentication Value 2 (JCB payment cards)
- CVC2 - Card Validation Code 2 (MasterCard payment cards)
- CVV2 - Card Verification Value 2 (Visa payment cards)

Cardholder Data Environment is the area of the computer system network that processes cardholder data or sensitive authentication data and those systems and segments that directly connect with or support cardholder processing, storage, or transmission. The PCI Compliance team is responsible for defining the scope of the cardholder data environment.

Change Management refers to the process of managing changes (e.g. additions, modifications, removals) to the production environment that could affect IT systems.

Cloud computing is a model for enabling on-demand network access to a shared configurable computing resource that can be rapidly provisioned and released with minimal management effort. For more information, reference NIST Definition of Cloud.

- Cloud capabilities: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)
- Cloud configurations: Private, Community, Public, and Hybrid (combines two or more configurations)

Confidential Information is business information that, if lost, disclosed, or inappropriately modified has a high potential to impact company reputation, strategies, operations, competitive advantage, financial performance, compliance, legal or regulatory obligations or information that can be used to identify a guest or team member.

Configuration Baseline is a set of specifications for a system or Configuration Item within a system.

Contractor is a person who is not a Target team member, but is engaged directly by Target or through a non-Target company to perform work on behalf of Target and has access to Target facilities and/or information assets (e.g., consultants, temporary workers).

Corporate Liable Device is a device that is purchased and paid for by the business.

Critical Logs refer to logs of events described in control CS-1557150 that are generated by critical systems (refer to Critical Systems).

Critical Security Patch is a patch that applies to installed functionality having an industry severity rating (CVSS – Common Vulnerability Scoring System) of 9.0 to 10 and vulnerability exploits identified as being available.

Critical Systems refers to hardware or software that share any of the following attributes:

- Are publicly accessible or internet facing (regardless of regulatory designation); or
- Deemed to be in scope for PCI (Payment Card Industry) and used to process, store and transmit Card Holder Data; or
- Contains or stores SHR data; or
- Covered by industry or government regulations including, but not limited to, systems in scope SOX (Sarbanes-Oxley Act), HIPAA (Health Information Portability and Accountability Act), and GLBA (Gramm-Leach-Bliley Act)

Cryptographic Key is a value that determines the output of an encryption algorithm when transforming plain text to cipher text, or vice versa. The length and cipher of the key generally determines how difficult it will be to crack the cipher text in a given message into plain text.

Data are facts or details that, by themselves, are rarely useful because they have no context, specificity, or organization.

Database refers to a structured format for organizing and maintaining easily retrievable information. Examples of simple database are tables and spreadsheets.

De-Identified Personally Identifiable or Protected Health Information refers to personal or health information that does not identify an individual and where there is no reasonable basis to believe that the information can be used to identify an individual.

Demilitarized Zone (DMZ) is a network area that sits between an organization’s internal network and an external network, such as the Internet.

Encryption is a method of converting plain text into an unreadable format with the use of an identified cryptographic key and encryption algorithm.

External Connections are attempts to join a device to the Target network. A successful connect will give that device access to Target network.

Financial Guest refers to a guest that has a continuing relationship with Target under which Target has provided a financial product or service that is used primarily for personal, family, or household purposes.

Financial Guest Personally Identifiable Information (PII) includes:

- Personal information provided by a guest (e.g., name, address, telephone number, Social Security Number (SSN), Social Insurance Number (SIN) or other unique identifier) in order to obtain a financial product or service
- Transactional information about the guest (e.g., account balance, payment history, overdraft history) involving a financial product or service
- Auxiliary information connected with providing a financial product or service to the guest (e.g., the guest’s status as a past or present guest, holds or held a financial product from Target, any information disclosure that indicates the guest is or has been a bank guest)

Firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.

Forensics is the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.

Functional Requirements refer to system feature and functions.

Gramm–Leach–Bliley Act (GLBA) requires financial institutions in the United States to create information security programs that ensure the security and confidentiality of guest (customer) information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of guest (customer) information that could result in substantial harm or inconvenience to any guest (customer).

Guest Payment Device (also known as Card Reader) is a device that captures payment card data via direct physical interaction with the card.

Health Insurance Portability and Accountability Act (HIPAA) is a national standard to protect the privacy of personal health information. The Act mandates the protection of Protected Health Information (PHI), and includes the requirements for documenting, handling, and protecting the privacy and security of medical records, medical billing, and patient accounts information.

Identity and Access Management (IAM) is the security discipline that enables the right individuals to access the right resources at the right time.

Inactive User Account is an account that has not been used in 90 days.

Information is the result of processing, organizing, structuring, or presenting data in a meaningful context so that it becomes useful.

Information Asset is a definable piece of information stored in any manner that is recognized as valuable to Target.

Information Processing Facilities house systems, services, or infrastructure. A facility can be either an activity or a place; it can be either tangible or intangible.

Information Resources are the data and information used or generated by Target, the systems, applications, devices, and facilities that store, transmit and process the information (e.g., laptop, email accounts, cell phones, software), and the personnel who use or consume the information.

Information Security is the act and condition of protecting information from unauthorized access, use, modification, recording, disruption, and destruction.

Information Security Agreement or Addendum (ISA) is an addendum to a non-disclosure agreement (NDA) that contains specific obligations describing when a vendor will: (a) handle personally-identifiable information about Target team members or guests; (b) connect to Target's information system or network; or (c) handle highly sensitive business information.

Information Security Event refers to any potential compromise to the confidentiality, integrity or availability of a Target information asset. Any issue that requires further investigation and tracking is classified as an event and may be elevated to an Incident, if warranted.

Information Security Incident refers to an event in which one of the following has occurred:

- Guest or Team Member notification is or may be triggered
- The compromise of an information asset has exposed internal or higher rated information to an external party
- The integrity of an information asset has been maliciously altered
- The availability of an information asset has been maliciously impacted

Information Security Requirements are requirements imposed on an information system, process, or facility that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Information Systems refer to Target's computer systems, containers, operating systems, network components, applications and services, including Application Programming Interfaces (APIs), and data stores.

Information Systems Owner is the Technology Owner that is responsible for the business delivery, functioning and services associated with the Information System. The Relationship Manager (*see Relationship Manager*) is considered to be the Information System Owner for systems provided by external vendors (*see Relationship Manager*).

Interactive Accounts refer to accounts that do allow for human interaction, either through allowing users to login to the accounts using a username or password, or allowing users to gain access to the accounts through any other type of configuration or system functionality.

Internal Information is business information for use by authorized team members and business partners during the normal course of conducting business or business contact information that can be used to identify a team member, intended for a limited audience who has a need to know the information or can also be designated for the entire organization where appropriate.

IT Systems - see Information Systems.

Least Privilege is the principle of allowing users or applications the least amount or permissions necessary to perform their intended function.

Malware is software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system.

Managed refers to the term used to describe how non-user account passwords are stored and managed within an approved enterprise password management tool. Non-user accounts are considered to be managed, when their passwords are automatically changed by an approved enterprise password management tool after use (*see Unmanaged*).

Media is a general term referring to the material onto which information has been recorded (e.g., paper, hardware, DVD, CD, thumb drive, USB flash drive, hard drive, tape).

Mobile Device is any portable device with internet capability, (e.g., laptop, tablet, smartphone).

Multi-Factor Authentication - *see Authentication.*

Non-Affiliate refers to any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with the organization.

Non-Critical Logs refer to logs of events described in control CS-1557150 that are generated by non-critical systems (refer to Critical Systems).

Non-Critical Systems refer to systems in scope for PCI that are not deemed to be critical systems (refer to Critical Systems).

Non-Disclosure Agreement (NDA) an agreement between two or more parties under which the parties agree not to disclose to others or misuse confidential information disclosed by one or more of the parties.

Non-Functional Requirements refer to system attributes such as security, reliability, performance, maintainability, scalability and usability.

Non-Interactive Accounts refer to accounts that do not allow for human interaction, either through allowing users to login to the accounts using a username or password, or allowing users to gain access to the accounts through any other type of configuration or system functionality.

Non-User Accounts are accounts that are leveraged by teams or applications for restricted access authentication and authorization. These accounts do not represent individual team members or contractors and can be divided into interactive (*see Interactive Accounts*) and non-interactive accounts (*see Non-Interactive Accounts*) based on how the accounts are accessed.

Password is any secret word, alphanumeric code, or passphrase that grants access to a restricted system or application.

Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card brands.

Penetration Tests are tests that attempt to find security weaknesses and identify ways to exploit vulnerabilities to circumvent or defeat security features of system components to gain access to system functionality and data.

Personal Device is a mobile device (e.g., iPhone, iPad, android phone/tablet) purchased by a team member for personal use that is also used to access Target data.

Personal Identification Number (PIN) is a unique authentication credential assigned to, or chosen by, an individual allowing the individual to access certain information.

Personal Information is any information that can be linked to an individual or used to identify directly an individual. Examples include name, social security number, race and mobile device ID.

Personally Identifiable Information (PII) is any information about an individual, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Platform Vulnerabilities are vulnerabilities that exist within the operation system, firmware, server based systems, database systems, Internet of Things (IOTs), ICS (Industrial Control Systems), and network components that support the application running within the platform).

Primary Account Number (PAN) is a unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. Also referred to as "Account Number".

Privileged Access provides the capability to change control parameters, program files, other users' access or configuration settings that can be used to bypass system or application security controls. These elevated rights include administrative privileges to workstations, servers, databases or applications, or broad, unrestricted application access. Privileged access must be restricted and assigned based on the principles of least privilege.

Product Boundary refers to a logical boundary associated with an IT system used to deliver or support a technology service.

Protected Health Information (PHI) is any individually identifiable health information held or transmitted by a covered entity or its business associate that relates to: (1) an individual's past, present or future physical or mental health or condition; (2) the provision of health care to the individual; or (3) the past, present or future payment for the provision of health care to the individual.

Public Information is information that that has been approved for public use or distribution.

Record refers to information that is created, received, and maintained as evidence of activities, decisions or agreements. Records are made or used in the normal course of business and may be physical or electronic. Records have information that provide evidence of compliance with internal or external requirements; quality of work or products; actions taken; decisions made; events that have occurred; transaction between two or more parties; contractual obligation between two or more parties.

Relationship Manager ("RM") (as defined in the Vendor Risk Management Policy) is the team member responsible for the day-to-day management of a Vendor through the Vendor life cycle.

The Relationship Manager is also considered to be the Information System Owner (*see Information System Owner*) for systems provided by external vendors and is responsible for ensuring that the vendor meets the security requirements defined within this policy.

Remote Access is access to information systems by a user (or an information system acting on behalf of a user) communicating through an external network.

Required Testing - see Testing.

Sarbanes-Oxley Act (SOX) is a U.S. federal law that set new or enhanced standards for U.S. public company boards, management, and public accounting firms, relating to the accuracy of financial information.

Secret is a logical or physical object used to protect the confidentiality of a given system or data from unauthorized individuals, entities or processes. Examples include passwords, certificates, connection strings, storage account keys, SSH keys, encryption keys, authorization tokens, license files, biometric data, etc.

Secure Coding is the process of creating and implementing applications that are resistant to tampering and/or compromise.

Secure Handling Required (SHR) information is information having such business and/or legal security or privacy requirements that call for additional controls beyond those defined within the Confidential category to meet compliance, legal or regulatory obligations.

Sensitive Authentication Data (SAD) is security-related information (including but not limited to card verification security codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Significant change is a change that impacts the security of Target's environment or the way in which we process, transmit or store data. These types of changes include but are not limited to the following categories:

- The introduction of large scale technology or infrastructure assets that are typically associated with a strategic change in business operations (examples of these types of changes include mergers and acquisitions, relocating data center operations or moving an application to a new technology platform)
- Changes to how we process, store and transmit data (examples of these types of changes include changing database types or changing network providers)

Single Sign-On (SSO) is a session and user authentication service that permits a user to login one time and gain access to multiple applications or other resources.

Strong Authentication - *see Authentication.*

Strong Cryptography is cryptography (encryption and hashing) that is designed and configured to protect data.

Strong Password is a password of sufficient length or compositional complexity that is hard to detect both by humans and by computers.

Systems - see *Information Systems***.**

Target Information is anything that concerns or relates to Target's business or anything that Target has a legal obligation to protect, including but not limited to, anything that is spoken, overheard, written, stored or communicated, copied, transmitted, held intellectually, or otherwise held tangibly or intangibly. Note: Team Member information is not meant to include wages, job descriptions, and other things relating to terms and conditions of employment. Nothing in the Information Security Policy, including the preceding definition of "information", is intended to restrict Team Members from discussing their wages, hours, working conditions, or any other terms and conditions of their employment.

Team Member includes employees of Target Corporation and its subsidiaries.

Testing refers to the verification and validation steps or procedures that are performed to confirm that the requirements have correctly been delivered.

Third Party refers to any person or business that does work on behalf of Target or provides products or services to but is not a Target team member and is not owned or operated by Target Corporation. Third parties include contractors, subcontractors, vendors, and service providers.

Threat is a condition or activity that has the potential to cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization.

Trusted Source refers to a party that appears to be trust worthy based on well-reasoned arguments and strong evidence in support of this status.

Two-Factor Authentication - *see Authentication.*

Unmanaged refers to the term used to describe how non-user account passwords are stored and managed within an approved enterprise password management tool. Non-user accounts are considered to be unmanaged, when their passwords are stored within an approved enterprise password management tool, however the account passwords are not automatically rotated by the tool after use (*see Managed*).

User is a person (team member, contractor, third party) who is granted access to use Target's systems.

User Accounts are information system accounts assigned to unique and specific people and that are used to authenticate to information systems. User accounts must not be shared between users.

Utility refers to utility system software designed to help analyze, configure, optimize or maintain computer systems.

Vulnerability is a flaw or weakness that, if exploited, may result in an intentional or unintentional compromise of a system.

Vulnerability Management is the process of mitigating or preventing the exploitation of technical vulnerabilities (Platform and Application level vulnerabilities) that may exist within an Information System. The process includes:

- periodically scanning or identifying of vulnerabilities
- investigating identified vulnerabilities
- assessing the severity and risk
- consulting and sharing the relevant information the appropriate team members
- reporting
- assisting with remediation, where appropriate

Wireless is a technology that permits the transfer of information between separated points without physical connection.