Security Standards Council®

Payment Card Industry (PCI)

Card Production and Provisioning

Physical Security Requirements

Version 2.0

December 2016

Document Changes

Date	Version	Author	Description
December 2012	1.x	PCI	RFC version
May 2013	1.0	PCI	Initial Release
March 2015	1.1	PCI	Enhancements for clarification
July 2016	2.x	PCI	RFC version
December 2016	2.0	PCI	Addition of Mobile Provisioning and other changes. See Summary of Changes from v1.1 to v2.

Table of Contents

1 Scope

The *PCI Card Production and Provisioning – Physical Security Requirements* manual is a comprehensive source of information for entities involved in card production and provisioning, which may include manufacturers, personalizers, pre-personalizers, chip embedders, data-preparation, and fulfillment. The contents of this manual specify the physical security requirements and procedures that entities must follow before, during, and after the following processes:

- Card Manufacturing
- Chip embedding
- Personalization
- Storage
- Packaging
- Mailing
- Shipping or delivery
- Fulfillment

In addition to the card production activities above this document defines the physical security requirements for entities that:

- Perform cloud-based or secure element (SE) provisioning services;
- Manage over-the-air (OTA) personalization, lifecycle management, and preparation of personalization data; or
- Manage associated cryptographic keys.

It does not apply to providers who are only performing the distribution of secure elements

Requirements for logical security for personalization are not included in this manual, but can be found in a separate document, *Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements*.

Unless prohibited by law, all entities undertaking any or all of the above activities must adopt the security control procedures and security devices specified in this manual as the minimum requirements accepted by the founding payment brands of PCI. Entities may adopt additional security controls as they deem appropriate, provided they are in addition to and enhance the procedures set forth in this manual.

Card production and provisioning entities management should review and recommend enhancements to the security procedures used by any contracted remote monitoring organization.

Appendix A: Applicability of Requirements makes further refinement at the requirement level for physical cards and mobile provisioning.

Although this document frequently states 'vendor', the specific applicability of these requirements is up to the individual payment brands; and the payment brand(s) of interest should be contacted for the applicability of these requirements to any card production or provisioning activity.

***Note:** All additional logical actions for vendors involved in personalization activities are detailed in the Logical Security Requirements document.*

1.1 Laws and Regulations

In addition to the physical security requirements contained in this document, there will almost certainly be relevant regional and national laws and regulations, including consumer protection acts, labor agreements, health and safety regulations, etc. It is the responsibility of each individual organization independently to ensure that it obeys all local laws and regulations. Adherence to the requirements in this document does not imply compliance with local laws and regulations.

If any of the requirements contained in this manual conflict with country, state, or local laws, the country, state, or local law will apply.

1.2 Loss Prevention

Vendors are responsible for preventing any unexplained product losses. Vendors are liable for any unexplained loss, theft, deterioration, or destruction of card products or components that may occur while such products are in the vendor's facility. Vendors are required to carry liability insurance covering all the risks stated above, taking into consideration the plant location, physical conditions and security of the plant, the number and duties of the employees, and the nature and volume of the contracted work.

1.3 Limitations

The individual payment brands are responsible for defining and managing compliance programs associated with these requirements. Contact the Payment Brand(s) of interest for any additional criteria.

2 Personnel

2.1 Employees

The following set of requirements applies to all employees that have access to card products, components, and the high security area (HSA).

2.1.1 Pre-employment Documentation and Background Checks

The vendor must undertake a pre-employment documentation and background check using the same pre-employment procedures, employment application documents, and background checks for:

a) Full-time employees

b) Part-time employees

c) Temporary employees, consultants, and contractors

d) Guards (internal or external)

2.1.2 Applicant/Employee Background Information Retention

The vendor must retain all applicant and employee background information on file for at least 18 months after termination of the contract of employment. This information must be available for the inspector during site security reviews.

2.1.3 Screening and Documentation Usage

2.1.3.1 Employment Application Forms

a) The vendor must use employment application forms that include the following detail relating to the applicant's past:

- Details of any "alias" or any other names.
- List of their previous addresses or residences for the last seven years
- Previous employers for the last seven years
- Applicants must satisfactorily explain gaps in employment.

b) The vendor must maintain a personnel file for each employee that includes but is not limited to the following information:

- Gathered as part of the hiring process:
  - Background check results
  - Verification of aliases (when applicable)
  - List of previous employers and referral follow-up results
  - Education history
  - Social security number or appropriate national identification number
  - Signed document confirming that the employee has read and understands the vendor's security policies and procedures
  - Fingerprints and results of search against national and regional criminal records

- Gathered as part of the hiring process and periodically thereafter:
  - Current photograph, updated at least every three years
  - Record of any arrests or convictions, updated annually
  - Annual credit checks

c) These files must be available to the security inspectors during site reviews.

2.1.3.2 Job and Sensitive Task Allocation – Restrictions

The vendor is responsible for determining the level of job responsibilities assigned to any temporary or interim staff (including consultants and contractors), except where the job function is restricted to employees.

2.1.4 Personnel Changes

2.1.4.1 Change in employee job function

The vendor must ensure that:

a) The security manager is notified in writing of any expected employee's job change prior to the change taking effect.

b) The security manager adapts the access control to restricted areas within one business day.

c) Where necessary, all combinations and other applicable access codes known to or utilized by employee are changed.

2.1.4.2 Termination of Employment

a) If termination of employment is a planned event, the security manager must be notified in writing prior to termination.

b) If termination of employment is an unscheduled event, the security manager must be notified in writing as soon as the decision is made.

c) Upon termination effective date of the employee the security manager or designated representative must:

- Deactivate all access rights.
- Recover the photo ID badge.
- Change all applicable vault combinations and other applicable access codes known to or utilized by employee.
- Recover all company property used in association with card production or provisioning.
- Verify completion of the employee termination checklist activities, below.

2.1.4.3 Termination checklist

The vendor must maintain a completed termination checklist on file confirming that staff members carry out the following procedures (where applicable) within one business day from the departure of the employee:

a) Disable or remove employee's computer user IDs and passwords from all applicable systems.

b) Retrieve all software programs and documentation distributed to employee.

c) Disable employee's access to computer data and applications.

d) Retrieve all company keys distributed to employee.

e) Retrieve employee's badge and photo identification and deactivate employee access to the facility.

f) Change all applicable vault combinations and other applicable access codes known to or utilized by employee.

2.1.5 Security Communication and Training

The vendor must emphasize security by:

a) Designating an individual (e.g., the CISO) responsible for all security matters and concerns, reporting to a senior company executive.

b) Ensuring that individuals performing or managing tasks requiring access to card components or data or support the cloud-based provisioning processes and/or environment have a signed employment agreement with the vendor. The agreement includes stipulating that the employee complies with company polices and rules.

c) Providing a copy of vendor's internal security manual to all employees and security personnel.

   The security manual must include the following sections:

   - Administration
   - HSAs
   - Security requirements and guidelines
   - Procedures that employees must follow while working in the secure facility
   - Specific requirements as they pertain to the cloud-based provisioning platforms and systems

d) Evidence of positive affirmation by the employee of receipt and understanding of responsibilities and obligations under the security policy.

e) Ensuring that vendor staff security training incorporates the obligation for employees to report any observed breaches of established security procedure.

f) Conducting mandatory training sessions at least annually. These sessions must include understanding the company security policies and the employees' responsibilities and their adherence to security policies.

g) Displaying posters and notices concerning security at key locations within the vendor facility.

h) Requiring that the individual with overall security responsibility reports to the board / Senior Executive Committee on a regular basis, preferably monthly, any security issues and the actions taken as a result.

2.1.6 Notification

The vendor must notify the Vendor Program Administration (VPA) of any personnel changes that directly affect the security of card products and related components, including but not limited to:

a) Senior management and corporate officers

b) Security manager

c) Employees authorized to receive or sign for any card components

2.2 Guards

2.2.1 *General Guidelines*

2.2.1.1 Prescreening

a) In-house or contracted guards must meet the same prescreening qualification requirements as employees working in HSAs.

b) The vendor must ensure that any guard service contracted from an outside source maintains liability insurance to cover potential losses.

2.2.1.2 Restrictions/Limitations

a) Guards are not permitted to perform any of the functions normally associated with the production of card products or card components.

b) Guards must not have access to:

- HSAs
- Employee records
- Physical master keys that provide access to card production or provisioning areas
- Audit logs
- Any restricted areas where the vendor processes, stores, or delivers card products and card components.

c) Guards must be prevented from modifying or altering the internal settings on access system controls, intrusion alarm system, closed circuit television (CCTV).

2.2.2 *Role and Responsibilities*

The guards' main role is to ensure permanent (at a minimum, during working hours) control of the security systems and maintain a high level of protection of the building, assets, access and staff, immediately reporting any discrepancy to the company. In addition, the vendor must ensure that:

a) Appropriate emergency procedures are followed and prompt attention to reports of unauthorized access to the premises is received from law enforcement agents, and where necessary the VPA

b) It maintains a clear segregation of duties and independence between the production staff and the guards.

c) Any time activities are performed in the HSA, the security control room is always occupied by at least one guard.

2.2.3 *Documentation*

The vendor must provide guards or any other person assuming the security functions outlined in this document with a copy of the vendor's internal security procedures manual, which at a minimum must include:

a) Guard’s responsibilities, procedures, and activities by position

b) Vendor’s security policies

c) Interaction between production process management, contracted guard or monitoring services, the police, and other emergency services

d) Access control at all entry and exit points of the premises, by date and time of activation

e) External resource response activities

f) CCTV monitoring and video or digital recordings

g) Administration of access cards and photo ID badges

h) Badge access system and computer monitoring (such as the logging in and out of staff entering or leaving the premises and internal movement at area access points)

i) Company policy concerning employee and visitor access to the facility (both exterior and interior)

j) Property removal

k) Shipping and receiving

l) Alarm activation procedures

m) Response to alarms, including notification to law enforcement in cases of unauthorized access to the premises

n) Daily activity and immediate incident report

o) Potential threats—such as burglary or theft—to the premises’ external or internal security

p) Handling of emergencies including but not limited to:

   - Fire
   - Earthquakes
   - Severe weather
   - Direct assault by armed felons
   - Bomb threats
   - Civil disturbances
   - Building evacuation
   - Ransom demands
   - Hostages
   - Kidnapping

q) The requirement that all guards, whether employees or contract, must sign a document indicating that they have read and fully understand the contents of this manual.

r) Procedures must be reviewed, validated and if necessary, updated annually.

2.2.4 *Security Training*

a) Guards must be trained and aware of all of their assigned tasks defined within the vendor's internal security procedures manual. Training must occur at least every 12 months and prior to the assignment of any new responsibilities. A record of the training session must be maintained.

b) Exceptional situations not specified within these manuals must be reported immediately to the security manager for appropriate action and possible inclusion into the manuals.

2.3 Visitors

a) Procedures for how visitors are managed at the vendor facility must be documented and followed.

b) All visitors to the facility must be registered ahead of their arrival.

c) The registration must include name and company they represent.

d) If the visitor requires access to the HSA or cloud-based provisioning environment, this must be approved by both the Security Manager and the Production Manager.

e) Any unsolicited visitors must be turned away.

f) An authorized employee must accompany all visitors at all times while they are in the facility.

g) Visitors must enter through the reception area.

2.3.1 Registration procedures

a) The vendor must apply the same registration procedures to all visitors entering their facility. These procedures must include the following:

- Confirmation of previously agreed appointment
- Verification of identification against an official, government issued picture ID

b) The vendor must maintain records, manually or electronically, of all visitors who enter the facility. If a manual logbook is used, it must contain consecutive, pre-numbered, bound pages.

c) All logs must be protected from modification.

d) The following information must be recorded in the logbook:

- Name of the visitor, printed and signed
- Number of the official ID document(s) presented and the date and place of issue
- Company the visitor represents (if any)
- Name of the person being visited or in charge of the visitor
- Purpose of the visit
- Visitor badge number
- Date and time of arrival and departure
- Signature of the employee initially assigned to escort the visitor

e) The vendor must retain visitors' registration records for at least 90 days.

2.3.2 Visitor Security Notification

At a minimum, the vendor must make visitors aware of vendor security and confidentiality requirements, and the vendor-provided escort must ensure the visitor's adherence to those requirements.

2.3.3 Visitor identification

a) Each visitor entering the facility must be issued with and must wear visibly on their person a security pass or ID badge that identifies them as a non-employee.

b) If the security pass or ID badge is disposable, the visitor's name and date of entry to the facility and, if multi-day, the validity period must be clearly indicated on the front of the badge.

c) If the security pass or ID badge is the access-control type that enables a record to be kept of the visitor's movement throughout the facility:

- The visitor must be instructed on its proper use.
- The vendor must program the visitor access badge or card to enable the tracking of movement of all visitors. It should be activated only for areas that the visitor is authorized to enter.
- Visitors must use their access card in the card readers to the room into which they enter.
- Badging to track access must be used wherever feasible.

d) Unissued visitor access badges must be securely stored.

e) Any un-badged access must be recorded in a log. Logs may be electronic and/or manual.

f) Employees responsible for escorting visitors while they are inside the facility must ensure that the visitor surrenders their ID badge to the receptionist or guard before leaving the building.

2.4 External Service Providers

2.4.1 General Guidelines

The vendor must ensure that:

a) Procedures that define how third parties are managed at the vendor facility are documented and followed.

b) The requirements of Section 2.1, "Employees," of this document have been met by the employer of all suppliers, repair and maintenance staff, and any other external service provider.

c) A pre-approved list of third parties is made available to the receptionist or to the guard on a daily or weekly basis for the preparation of ID badges. Only those persons with pre-approved ID badges may be granted facility access. The security manager or senior management must approve in writing any exceptions to this requirement.

d) An employee accompanies all external service providers at all times while they are in the HSA(s).

e) All external service providers that require access to HSAs to service equipment have adequate liability insurance.

f) External service providers' staff requiring access to restricted or HSAs follow the visitor-registration procedures.

2.5 Vendor's Agents

2.5.1 General Guidelines

a) Prior to conducting any business with an agent or third party regarding card-related activities, the vendor must register the agent with the VPA and obtain the following information:

- Agent's name, address, and telephone numbers
- Agent's role or responsibility

b) The vendor must inform the VPA whenever the agent relationship is changed or terminated.

c) Agents of the vendor are not permitted to be in the possession of a card(s), card components, or card personalization data.

3 Premises

3.1 External Structure

3.1.1 External Construction

a) Procedures for security controls implemented at the vendor facility must be documented and followed.

b) The vendor must prevent unauthorized access to buildings, building areas, or structures containing technical machinery or equipment such as the heating system generator, auxiliary power supply, and air conditioning.

c) The vendor must protect doors that provide access to these by use of electrical or magnetic contacts that are permanently alarmed and that are connected to the security control-room panels.

d) The vendor must establish a specific procedure to disable these door alarms and to control the delivery of the access key any time that repair or maintenance staff must access this machinery or equipment.

e) The vendor must keep a log of the disabling of the alarm and the key exchange, describing at least:

- Date
- Time
- Person(s) needing access
- Purpose of the access

3.1.2 Exterior Entrances and Exits

All non-emergency exterior entrances and exits to the facility must be:

a) Contact-alarm monitored

b) Locked or electronically controlled at all times

c) Reinforced, where applicable, to resist intrusion (e.g., steel or equivalent construction that meets local fire and safety codes)

d) Fitted with an access-control device (i.e., card reader or biometric) that automatically activates the locking mechanism

e) Fitted with a mantrap or interlocking configuration to prevent staff “piggybacking” or tailgating (excluding emergency exits)

3.1.3 External Walls, Doors and Windows

a) All exterior walls must be pre-cast or masonry block or material of equivalent strength and penetration resistance.

b) Windows, doors, and other openings must be protected against intrusion by mechanisms such as intruder-resistant (e.g., “burglar-resistant”) glass, bars, glass-break detectors, or motion or magnetic contact detectors.

3.1.4 Building Peripheral Protection

The vendor must not place any device (e.g., carriers, waste containers, and tools) against the external wall protecting the outer perimeter of the vendor's facility.

3.2 External Security

a) The vendor premises must be located in an area serviced by public law enforcement and fire protection services in a timely manner.

b) The facility must be secured with an intrusion alarm system as defined in Section 3.4.1, "Alarm Systems."

c) The alarm system must be equipped with an auxiliary power or battery backup system with capabilities for ensuring operation for a minimum of 48 hours in the event of a power failure.

d) All systems must notify the vendor in real time in the event the backup system is invoked.

e) All external entry and exit points, including those for freight and maintenance, must be equipped with a peep-hole, a security window, or external CCTV that allows security personnel visual inspection of the immediate area, thus allowing action to be taken in the event of unauthorized access.

f) Alarms on external doors must be tested every three months.

3.2.1 Emergency Exits

a) All emergency exits must be fitted with local audible alarms and monitored 24 hours a day and also must display a sign indicating "emergency exit door with alarm."

b) Emergency exit doors must be fitted with an automatic closer to ensure self-latching of the door after being opened.

c) Emergency exit doors must be contact-alarm monitored.

d) These doors must be used only in the event of an emergency and not used for any other purpose.

e) During working hours, either the internal security control room or staff at a central monitoring service center must receive the signal from the emergency exits.

f) During non-business hours, the activation of an emergency-exit alarm must summon the local police or a guard response directed by central monitoring service or on-site security control.

g) Emergency exit doors must not be capable of being opened from the outside.

h) Emergency exits must not lead to a higher security area.

3.2.2 Exterior Lighting

a) Exterior lights must illuminate the exterior of the facility as well as all entrances and shipping and delivery areas, such that persons within these areas can be identified.

b) The vendor must check all exterior lights monthly and must maintain a record for 24 months.

3.2.3 Roof Access

a) Trees, telegraph poles, fences, etc. located adjacent to the property line that might facilitate roof access must be removed, relocated, or otherwise secured against unauthorized access.

b) All access points into the building from the roof must be locked or otherwise controlled from the inside.

c) All access points must have magnetic contacts or contact sensors both of which must have monitored access.

d) All skylights, ventilation, and cooling system ducts that penetrate the building structure must be secured with security mesh, grating, or metal bars to prevent unauthorized access.

3.2.4 Exterior CCTV

a) Exterior CCTV cameras must focus on all entrances and exits to the building, and capture legible images of all persons entering or leaving the facility.

b) Cameras must be monitored in the security control room during operational hours.

3.2.5 Signage

Signage on the exterior of the building must neither indicate nor imply that the vendor processes card products.

3.3 Internal Structure and Processes

3.3.1 Reception

a) The main entrance to the building must lead visitors into a reception area that restricts any physical contact between visitor(s) and the receptionist/guard.

b) The reception area must be contained within a mantrap.

A mantrap is the secured space between doors operating on an electronic interlocking basis that may be accessed by a card-reader access system or a remote-control device, provided that all movement and activity is monitored.

c) The receptionist or guard responsible for the entrance and departure of visitors must have an unobstructed view of the reception area at all times.

d) Visitors must be visually inspected in this area to confirm their identity and issued with identification badges before being admitted into the facility.

e) The vendor must maintain a list at reception of all staff authorized to bring visitors into the vendor facility. Only people on the list are allowed to bring visitors into the facility.

f) Visitors must only be allowed access beyond the reception area after identification has been established and the appropriate ID badge issued, which must be worn by the visitor at all times whilst inside the facility.

g) The electronic control points for operating this system must be located at the receptionist’s desk or in the security control room.

h) If the control points for operating the external doors are located at the receptionist's desk, the wall(s) separating the receptionist area from the reception room must be reinforced and fitted with a security window—i.e., a window of bullet-resistant transparent material containing a slot or device that allows the transfer of small packages and documents from the reception area to the receptionist or security guard.

i) The vendor must provide employees working in these areas with a telephone and a duress button that activates a silent alarm at a remote, central monitoring service or police station.

j) If the receptionist area houses or acts as a security control room, the requirements as defined in Section 3.3.2, "Security Control Room," must be met.

k) Outside working hours, all security protection devices (including alarm activation and deactivation) must be monitored electronically by either an in-house security monitoring system or a private central monitoring company.

l) Employees may enter the facility through the main entrance area or through an employee-only entrance. The external entrance door of the building must not lead directly to the entrance of the HSA or the cloud-based provisioning area.

3.3.2 Security Control Room

3.3.2.1 Definition

This is the room housing the primary CCTV monitoring systems, intrusion, fire, and alarm-system control and access-control systems.

3.3.2.2 Location and Security Protection

The vendor must:

a) Staff the room at all times while activity occurs in the HSA

b) Locate the security control room outside of the HSA and cloud-based provisioning environment to achieve the segregation of duties and independence between the guards and the HSA staff.

c) Build the security control room of concrete block or other material offering similar resistance, if not part of the facility.

d) Protect the room by an internal motion detector.

e) Fit the door giving access to the room with an in and out card reader access system plus an anti-pass-back software function connected to a computer that records all accesses and exits.

f) Ensure that the software counter registering the in and out card transactions in the access-control system logs the card transactions at the end of an access cycle (activation of the card reader with the access card, opening and closing of the door).

g) Calibrate the security control room movement detector to generate an alarm if movement is detected inside the room when the software counter is zero (nobody registered in the room). The vendor must also calibrate the movement detector to generate an alarm if no movement within fifteen or fewer minutes is detected inside the room when the software counter is equal or greater than one (at least one person registered inside the room).

h) Ensure that in both above scenarios the alarm is both locally audible and that an alarm must be sent directly to the alarm monitoring services (security control room and the external security company or police station).

i) Fit the door with an automatic closing device. The opening of the door for more than 30 seconds must automatically activate a sound alarm. The access-control system must be programmed, whereby access is on a person-by-person basis and restricted to authorized personnel only. Person-by-person access may be fulfilled through a procedural control.

j) Ensure that each individual entering or exiting completes the full cycle of badging in and badging out.

k) Equip the security control room with two independent means of communication.

l) Ensure that the badge access-control monitor permanently displays the access card transactions on a real-time basis. Guards must be able to cross-check the access-control records with the CCTV images.

m) Train guards in the security control room in the effective use of badge access-control system and CCTV system facilities.

n) Ensure that a security guard is assigned to watch all real-time CCTV images on the monitors.

o) Equip the room with a bullet-resistant security window facilitating the exchange of keys and documentation between the security control staff and external visitors or HSA staff while minimizing physical contact and access to unauthorized staff.

p) Equip any other external-facing windows with bullet-resistant glass and mirror filming sufficient to prevent any observation from outside the building.

q) Have mechanisms in place to prevent observation of security equipment (e.g., CCTV monitors) inside the security control room—for example, by covering all security control room windows with a one-way mirror film or other material preventing viewing from outside.

r) Ensure all other windows within the security control room are protected by unbreakable glass or iron bars and are protected against intrusion by at least one of the following: burglar-resistant glass, glass-break detectors, or motion or magnetic contact detectors.

s) Ensure that when the room is used for reception control, the conditions outlined in Section 3.3.1, "Reception," apply.

t) The CCTV and access control servers must be in the security control room or a room with equivalent security. The servers must not be in the HSA.

3.3.3 High Security Areas (HSAs)

3.3.3.1 Definition

Areas in production facilities where card products, components, or data are stored or processed are called high security areas. Only card production and provisioning-related activities shall take place within the HSA. At a minimum, the following activities must take place only in an HSA:

- Card manufacturing
- Chip embedding
- Personalization
- Storage
- HCE and SE mobile provisioning
- Packaging
- Mailing
- Shipping or delivery
- Fulfillment

a) Employees may only bring items related to card production and provisioning activity into the HSA.

b) If a facility performs multiple production activities—e.g., card manufacturing and personalization—these activities must be performed in separate areas within the HSA.

c) With the exception of mobile provisioning, if multiple HSAs are within the same building, they must be contiguous.

d) Equipment that is purely associated with test activities is not allowed in the HSA.

e) A mobile provisioning system must exist in either a server room in the HSA or, if the only activity by the vendor, its own room meeting the criteria for an HSA.

3.3.4 HSA – Security Protection and Access Procedures

3.3.4.1 Access Control

a) Access to the HSA must be restricted to authorized persons through an access-control system, working on a strict person-by-person basis.

b) Access-control systems must:

- Always be connected to the computer that monitors and logs all staff and visitor movements.
- Prevent employees from piggybacking.
- Enforce person-by-person access.
- Implement anti-pass-back mechanisms.
- Enforce dual presence. If the number of authorized employees is less than two for more than a minute, the alarm must be activated.

c) The vendor must program the software access-control system, whereby access is on a person-by-person basis and restricted to authorized personnel.

d) The access-control system must activate the alarm system each time the last person leaves the HSA.

e) The HSA and all separate rooms within the HSA must be protected by internal motion detectors, even if no production occurs in the room.

f) The motion detector must generate an alarm if movement is detected inside the HSA or rooms within the HSA when the access-control system indicates (e.g., the software counter is zero—nobody registered in the room) the room is not occupied.

g) The warning must be a local sound alarm and notification (silent alarm) within the security control room. Additionally, after working hours, a simultaneous alarm to the local external security company or local police must occur.

h) No one is allowed to bring personal items (for example, packages, lunch containers, purses) or any electronic devices (including but not limited to mobile telephones, photo cameras, and PDAs), into the high security area. Medical items such as medications and tissues are acceptable if in clear containers that can be examined. No food or beverages are allowed.

i) If the access-control server is not located in the security control room it must be located in a room of equivalent security. The access-control server cannot be located in the HSA

3.3.4.2 Person-by-Person Access Control and Anti-pass-back Software Function

a) Access must be enforced by the use of an air lock, single sluice, or security turnstile, which must be controlled by logical means, ensuring strict compliance with the person-by-person mandate.

b) Activation of the access device must be controlled by a card reader that enforces an anti-pass-back function.

c) The card readers must be permanently connected to a computer that centralizes the logging of any card reader activation.

d) The status of the access must change only when the person has successfully completed the access cycle.

3.3.4.3 Transfer of Materials

a) All materials required for production must be transferred to the HSA through either a goods-tools trap or the shipping and delivery area.

b) A goods-tools trap may be used to transfer materials between different areas within the HSA.

3.3.4.4 Security Controls

a) Bullet-resistant (e.g., UL 752) glass or iron bars must protect all windows in HSAs.

b) It must not be possible to view activities in the HSA from the exterior of the building — e.g., by use of opaque or non-transparent glass.

c) Walls and ceilings must be constructed around the HSA consistent with the enforcement of dual presence—e.g., prevention of access via false ceilings or raised floors.

d) All access points (e.g., electrical conduits, opening windows and ventilation shafts) in HSAs must have physical barriers.

e) Windows are not permitted to be opened. Windows that are openable windows must additionally be fitted with contact monitors to detect the opening of the window in order to prevent card components from being passed through the windows.

f) The entire HSA must be covered by CCTV as defined in Section 3.4.5, "Closed Circuit Television (CCTV)."

g) All doors and gates to these areas must be contact monitored and fitted with automatic closing or locking devices and audible alarms that sound if the door or gate remains open for more than 30 seconds.

h) All doors must be fitted with an in and out card reader access system plus an anti-pass-back function connected to a computer that records all movements.

i) Doors must not open directly to the building's exterior unless they are alarmed emergency exit doors.

j) Emergency exits must be fitted with local audible alarms and monitored 24 hours a day and also must display a sign indicating "emergency exit door with alarm."

3.3.4.5 Minimum Number of Persons

Whenever any room within the HSA is occupied, it must contain a minimum of two authorized employees. This must be enforced by the access-control system.

3.3.5 Rooms

a) Separate rooms within the HSA must meet all of the HSA requirements with the exception of person-by-person access.

b) Toilet rooms are prohibited except where required by local law. Where used, the entry/exit way must be camera-monitored.

c) If the HSA contains fire doors and these doors are normally closed or can be manually closed, then these doors are subject to the same access controls as any other door that provides access to a room.

d) If the HSA contains fire doors and these doors are locked open and only closed automatically when a fire alarm is activated, then the access controls that normally apply for accessing a room do not apply.

Within the HSA, the following separate rooms may exist:

3.3.5.1 Pre-Press Room

a) The pre-press process must be performed in a separate room within the HSA.

b) The pre-press room is where the vendor produces or stores film, plates, or electronic media.

3.3.5.2 Work in Progress (WIP) Storage Room

a) This room must be segregated from production and protected at a minimum by wire mesh.

b) If wire mesh is used in the construction of such areas, it must extend from the floor to enclose the entire room on all surfaces, including a top (if below the ceiling).

c) Doors to these areas must be contact monitored and fitted with an audible alarm that sounds when the door remains open for more than 60 seconds.

d) Reinforced exterior walls may be used as part of the perimeter of these areas provided that these walls do not contain any door(s) or window(s).

e) CCTV surveillance is mandatory and must cover the entire area, ensuring that there are no blind spots.

3.3.5.3 Card Product and Component Destruction Room(s)

a) Destruction of card product and component waste must take place in a separate room(s) within the HSA that is dedicated for destruction.

b) Destruction by a third party may take place in the loading bay using portable/mobile equipment. All requirements for a destruction room must be met for this temporary usage.

3.3.5.4 PIN Mailer Production Room

a) PIN mailer production must be performed in a separate room within the HSA.

b) Employees involved in personal identification number (PIN) printing and mailing processes must not monitor or be involved in the personalization, encoding, and embossing of the related cards. Individuals may perform other non-personalization activities in addition to PIN printing, except for those that give access to cardholder data such as data administration, packaging, or mailing activities.

c) Personnel involved in personalization must never be involved in PIN printing of the associated cards. Defined procedures must demonstrate that these personnel are not involved in the production of the associated cards.

d) PIN mailers must be printed in such a way that the plaintext PIN cannot be observed until the envelope is opened. The envelope must display the minimum data necessary to deliver the PIN mailer to the correct customer. PIN mailers must be tamper evident so that it is highly likely that accidental or fraudulent opening will be obvious to the customer.

e) PIN mailers must be mailed as defined in Section 5.4, “Delivery.”

f) No activity other than PIN mailer production may take place in the room.

g) All re-runs of jobs to print PINs must be pre-approved in writing by management.

h) Reports and PIN mailers must not display printed PIN data in the clear.

i) PIN mailers must not contain the associated cardholder account number

j) PIN mailers must be stored in the vault or the PIN printing room prior to shipment.

k) All waste material from the PIN printing process must be destroyed as defined in Section 4, “Production Procedures and Audit Trails.”

3.3.5.5 Server Room & Key Management Room

a) Server processing and key management must be performed in a separate room within the personalization HSA. Data preparation must occur here. Server processing and key management may occur in the same room or each in a separate room

b) Systems and applications that make up the cloud-based provisioning network must be physically segregated from other vendor networks and internet-connected networks. This includes separation of servers, firewall, and HSM. For example, in a traditional card vendor environment this could be a separate rack in a server room, or in a provisioning-only entity, housed in a separate room or cage in a data center. It cannot be in the same rack as other servers used for different purposes.

c) An internal CCTV camera must be installed to cover the access to this room and provide an overview of the room whenever there is activity within it. The camera must not have zoom or scanning functionality and must not be positioned in such a manner as to allow observation of keystroke entry or the monitoring of the screen.

3.3.5.6 Vault

The vault is the primary security area in the vendor facility.

a) The following must be stored in the vault:

- Cards awaiting personalization
- Security components
- Materials awaiting destruction
- Samples and test cards prior to distribution and after return
- Any card that is personalized with production data
- If the facility is closed, personalized cards that will not be shipped within the same working day
- Products awaiting return to the supplier

b) Vaults must be constructed of reinforced concrete (minimum 15 centimeters or 6 inches) or at least meet the Underwriters Laboratories Class I Burglary Certification Standard (e.g., UL 608), which provides for at least 30 minutes of penetration resistance to tool and torch for all perimeter surfaces—i.e., vault doors, walls, floors and ceilings.

- An outside wall of the building must not be used as a wall of the vault.
- If the construction of the vault leaves a small (dead) space between the vault and the outside wall, this space must be constantly monitored for intrusion—e.g., via motion sensors.
- No windows are permitted.
- There must be no access to the vault except through the vault doors and gate configurations meeting these requirements. The vault must be protected with a sufficient number of intruder-detection devices that provide an early attack indication (e.g., seismic, vibration/shock, microphonic wire, microphone, etc.) on attempts to enter and also provide full coverage of the walls, ceiling, and floor.
- The vault must be fitted with a main steel-reinforced door with a dual-locking mechanism (mechanical and/or logical—e.g., mechanical combination and biometrics) that requires physical and simultaneous dual-control access. The access mechanism requires that access occurs under dual control and does not allow entry by a single individual—i.e., it is not feasible for a single individual to use credentials belonging to someone else to simulate dual access.

c) Opening of the main vault door must always be under dual control requiring two authorized staff to be simultaneously present and involved in the opening and closing of the door.

d) If the vault door is required to remain open during production hours, an inner grille must be used. The vault door or inner grille must remain closed and locked at all times, except when staff require access to the vault for example to store or remove items. The inner grille must meet the same access-control criteria as other rooms within the HSA.

e) The vault door or the inner grille must be equipped with an automatic closing device and must automatically activate a simultaneous sound alarm, locally and in the security control room, if opened for more than 60 seconds.

f) Emergency exit doors from the vault to the HSA must meet the strength requirements for a vault door, must be alarmed and not capable of being opened from outside, and must conform to the requirements for emergency exits.

g) Card components being taken in or out must be recorded in a vault log and confirmed by at least two employees.

h) Maintenance of these audit control logs is mandatory as defined in Section 4.7.2, "Vault Audit Controls." These logs must be retained for the longer of five years or the oldest card in the vault.

i) If the vault also is used to store non-payment products, it must be physically segregated (e.g., stored on dedicated aisles or shelves) to create a physical separation between payment products and other card types.

j) All boxes with payment cards must have a label, visibly attached, describing the product type, a unique product identifier number, the quantity of cards contained in the box, and the date of control.

k) Unsealed boxes are only permitted for stock that requires multiple pulls per day. Unsealed boxes must be in a centralized area within the vault. The counting process must be applied during the pull process, and an inventory count under dual control must be performed for each unsealed box at the end of each shift. All other boxes must be sealed.

l) Vault storage must be organized so that it is possible to identify the location of any stock item within the vault.

m) CCTV surveillance is mandatory and must cover the entire area, ensuring that there are no blind spots.

3.3.6 Other Areas

3.3.6.1 Goods-tools Traps

Goods-tools trap configuration options are as follows:

a) One-room configuration

The goods-tools trap is composed of a unique, closed, solid construction room (goods transfer room) and two doors (inner and external) minimizing the physical contact between the individuals collecting or delivering materials and the HSA staff.

In this configuration, the goods-tools trap must be operated as follows:

- The movement detector is deactivated when someone swipes the access card in the card reader.
- The person opens the door, introduces the package, and closes the door.

  - The movement detector is reactivated automatically, so any person inside the goods-tools trap is detected. If someone is detected, the cycle cannot be completed, and the other goods-tools trap door cannot be opened to take the package back.
  - If no motion is detected in the trap, and the first door has been closed, the second door in the HSA can be opened for someone to take the package.

b) Two-room configuration

In this configuration, the goods-tools trap is composed of two consecutive rooms, similar to the classical shipping and delivery room configuration.

Security requirements, protection devices, and access procedures are the same as for the standard shipping and delivering area configuration, as defined below.

3.3.6.2 Shipping and Delivery Areas

a) To facilitate the shipment and delivery of card components, the loading/unloading area must be composed of at least two consecutive enclosed rooms and three doors (external, intermediate, and inner), which minimizes physical contact between the individuals collecting or delivering materials and the shipment/delivery employees and card production staff.

b) All shipping and delivery doors must operate on an electronic and interlocking basis so that when one of the doors is open the others are electronically locked.

c) An intercom communications system must be contained in this area to allow identification of incoming drivers.

d) One of the rooms in the shipping area must contain a solution to allow the exchange of control documents without coming into contact with external personnel, as well as being able to communicate with and visually identify them—e.g., a security window, video intercom, CCTV monitors etc.

e) The inner shipping/delivery area door must have access control installed to restrict access to authorized users and to record usage. The logging at a minimum must include each opening and closing of the door.

f) The guards may operate the external door of the outer room area only after the driver is identified and the production staff is informed about the ongoing shipment or delivery operation. To prevent unauthorized access to the HSAs through the shipping and delivery rooms, the inner room must be protected by an internal movement detector that prevents the opening of the internal door and the intermediate door of the inner room if movement is detected inside this inner room.

g) An alarm must be generated automatically and logged in the central alarm system, and all shipment and delivery area doors must be blocked each time movement is detected by the movement detector located inside the inner room when the intermediate and inner doors are both closed and locked.

h) To liberate a person detected inside the room and stop the alarm, the software monitoring the access-control system must only allow the opening of the last activated door. A logical (software) and physical (alarm report book) log of the event must permanently be kept.

i) The vendor must install CCTV cameras and orient the cameras to cover the external and inner access doors to the shipping and delivery areas, and capture all activities during shipping and delivery operations.

j) The vendor must install at least:

  - One external CCTV camera covering the external shipping and delivery area door and its environment
  - Two CCTV cameras inside the outer room covering all sides of the vehicle
  - One CCTV camera inside the inner room covering the shipping and delivery operations

k) The images captured and recorded by these CCTV cameras must be displayed on the security control room monitors in real time, allowing the guards to control the shipping and delivery operations.

l) These images must also be displayed on a monitor located beside the security window, allowing the production staff to oversee the shipping and delivery operations.

3.4 Internal Security

3.4.1 Alarm Systems

a) To alert personnel working in the vicinity of and in the security control room, local alarms or flashing lights must activate when a door or gate to a restricted area is left open for more than 30 seconds except where otherwise specified in this document.

b) The alarm system must be protected by an auxiliary power or battery backup system with capabilities for ensuring operation for a minimum of 48 hours in the event of a power failure.

c) The system must notify the vendor in real time in the event the backup system is invoked.

d) The alarm activation and deactivation must be checked and confirmed by an electronic device, guards, private security company, or local police force to ensure that the pre-arranged alarm time settings have been respected. The alarm deactivation process must allow for the generation of a fast, silent alarm in case of threat.

  - A specific procedure must be established to ensure quick corrective action in case an alarm is not activated in accordance with pre-arranged alarm time settings.
  - Alarm activation and deactivation codes must be known only by the employees authorized to use them.
  - Guards and employees must follow these procedures in case of alarm system activation. These procedures must be clearly described and included in the internal security procedures manual.

e) Access contacts and motion detectors must be activated in zones where no staff are present (e.g., vault, storage, production areas, shipping and delivery areas).

3.4.2 Badge Administration

3.4.2.1 Identification badges

a) Procedures must be documented and followed for managing identification (ID) badges.

b) The vendor must issue a photo identification (ID) badge to each employee.

c) The ID badge must not be imprinted with the company name or logo.

d) Access credentials (which may be the ID badge) must be programmed only for the access required based on job function.

3.4.2.2 ID Badge or Access Card Usage

a) The access-control system must grant physical access to employees only during authorized working hours, and only to those areas required by the employee's job functions.

b) Employees must display their ID badges at all times while in the facility.

c) Employees are responsible for their ID and access badges and must report any lost/ stolen or broken badges to the Security Manager immediately.

d) The audit logs of the ID badge access-control system changes and exception conditions must be reviewed weekly to ensure badge assignments are appropriate and the system is functioning appropriately.

3.4.2.3 ID Badge or Access Card Inventory and Management

The security manager is responsible for unassigned ID badges and must:

a) Maintain an inventory of unassigned ID badges.

b) Ensure dual control exists for badge access and assignment.

c) Ensure ID badges are retrieved from terminated employees prior to their departure from the premises.

d) Ensure all access rights are immediately deactivated.

e) Maintain precise documentation accounting for all lost badges.

3.4.3 Badge Access System

a) The vendor must document, follow, and maintain procedures for ID badge administration.

b) Badge access systems that allow entry into restricted areas must have a backup electrical power source capable of maintaining the system for 48 hours.

c) Contingency plans must exist for securing card components in the event of an outage greater than 48 hours.

3.4.3.1 Activity Reports

a) All procedures for badge access must be documented and kept current.

b) The badge access system must log sufficient information to produce the daily card activity reports detailed below:

  - Card reader
  - Card reader status
  - Card identification
  - Date and time of access
  - Access attempts results
  - Unauthorized attempts
  - Anti-pass-back violation and corrective actions taken

- Badge access system changes describing:
  i. The date and time of the change,
  ii. The reasons for the change, and
  iii. The person who made the change.

c) The security manager must review these reports weekly.

d) The badge access system audit trail must be maintained for at least three months.

3.4.3.2 System Administration

The vendor must ensure that:

a) Each badge access system administrator uses his or her own user ID and password.

b) Passwords are changed at least every 90 days.

c) User IDs and passwords are assigned to the security manager and authorized personnel.

d) The security manager and other authorized personnel are the only individuals able to modify the badge access system controls. All changes to the system must be logged.

e) At the end of each session, the individual who initiated the session must log off the system.

f) All changes to card production, provisioning and security-relevant systems are recorded and reviewed monthly by a senior manager who is not the individual initially involved in changing the system.

g) Systems administration (this does not include badge administration) must follow the requirements for onsite remote access if performed remotely. Vendor facilities that are not subject to logical security audits must confirm in writing that the following requirements are met:

h) Badge access systems are isolated on a dedicated network from the main office network.

i) Offsite access to the badge access system is not permitted.

j) Access-control system data must be backed up on a weekly basis.

k) Access-control systems administration must be performed from within the security control room.

l) For generic administrative accounts that cannot be disabled, the password must be used only for emergency. The password must be changed from the default value and managed under dual control.

m) In addition, the access control system must meet the logical security requirements in Appendix B.

3.4.4 Duress Buttons

3.4.4.1 Location

Duress buttons must be located in the following areas:

a) Reception,

b) Security control room

c) The vault

d) Shipping and delivery area

e) Every employee entrance

3.4.4.2 Activation

a) When a duress button is activated, a warning or emergency signal must be sent to the security control room, a remote central monitoring station, or the local police station. The anticipated initial response (i.e., event verification) must be within two minutes.

b) All details relating to the activation of the duress button and the response by the remote central monitoring service or the local police must be recorded in the control log, including the following:

- Time and date when the duress button was activated
- Time taken by the remote central monitoring service to respond
- Time taken by the police or other help to respond/arrive on site
- Chronology of all related activities, including names of personnel involved
- Reason for activating alarm

3.4.4.3 Testing

All duress buttons must be tested and the results documented on a quarterly basis.

3.4.5 Locks and Keys

3.4.5.1 Key Receipt and Return

The term ”key” as used below refers to any physical key or combination giving access to a restricted area, including those inside the HSA or cloud-based provisioning area.

a) Procedures for managing keys must be documented and followed

b) Employees who are issued keys must sign a consent form indicating they received such keys and that they will ensure that the key(s) entrusted to them cannot be accessed by unauthorized individuals.

c) All unissued keys, master keys, and duplicate keys must be maintained under dual control in a safe or secure cabinet.

d) Any transfer of responsibility between the staff issuing the key and the key recipient must be recorded in a specific key logbook.

3.4.5.2 Audits and Accountability

a) The key logbook must have consecutive, pre-numbered, bound pages and must contain at least the following information:

- Key identification number
- Date and time the key is issued (transfer of responsibility)
- Name and signature of the employee issuing the key
- Name and signature of the authorized recipient
- Date and time the key is returned (transfer of responsibility)
- Name and signature of the authorized individual returning the key
- Name and signature of the employee receiving the key

b) If an electronic system is used to control access to keys, that system must be administered under dual control and be able to produce a report with equivalent information.

c) For keys that allow access to sensitive materials, the security manager must conduct a quarterly review of:

- The key logbook
- The list of employees authorized to hold keys
- The locks each key operates

d) The security manager must sign and date each of the key control documents, attesting that the review process was completed.

3.4.5.3 Master Keys

The security manager and executive managers are the only employees authorized to possess master or overriding keys to restricted areas.

3.4.5.4 Safe and Vault Combinations

Combinations for any combination locks where a combination holder had access must be changed when a combination holder is removed from the list of authorized combination holders.

3.4.6 Closed Circuit Television (CCTV)

3.4.6.1 CCTV Cameras

a) Procedures for managing the facility’s CCTV must be documented and followed.

b) All CCTV cameras must be tested, and the images displayed by the monitors checked for clear visibility at least monthly. The vendor must maintain a record of such testing on file for a minimum of two years.

c) In case of CCTV involuntary or voluntary disconnection, the “video loss” clicking box displayed by the monitors located in the security control room must be accompanied by a sound alarm.

d) Both the digital recording and access-control systems must be synchronized with real time. The synchronization of the systems must be within two seconds of one another.

e) The recording system must be able to replay any recorded sequence without stopping the normal recording operation.

f) CCTV cameras in server rooms and PIN-mailer rooms must not contain (or must have disabled) zoom or scanning functionality.

3.4.6.2 Monitor, Camera, and Digital Recorder Requirements

a) Each monitor, camera, and digital recorder must function properly and produce clear images on the monitors without being out-of-focus, blurred, washed out, or excessively darkened. The equipment must record at a minimum of four frames per second.

b) CCTV cameras must record all activity, including recording events during dark periods through the use of infrared CCTV cameras or automatic activation of floodlights in case of any detected activity. This recording may be via motion activation. The recording must capture any motion at least 10 seconds before and after the detected motion.

c) CCTV monitors and recorders must be located in an area that is restricted from unauthorized personnel.

d) CCTV cameras must be connected at all times to:

- Monitors located in the control room
- An alarm system that will generate an alarm if the CCTV is disrupted
- An active image-recording device

3.4.6.3 View Requirements

a) Each camera view must include all activities necessary to provide adequate security coverage. Blind spots must not exist.

b) The recording must capture sufficient images to identify the individual (e.g., head and shoulders view) as well as the activity being performed.

c) Each internal CCTV camera and recording system must be equipped with an automatic recording capability in case of an alarm event.

3.4.6.4 Retention of Video Recordings

a) CCTV images must be kept for at least 90 days and must be backed up daily. Both primary and backup copies must exist for a minimum of 90 days.

b) The backup recording must be stored in a separate, secure location within the facility and must ensure segregation of duties between the users and administrators of the system. Backups may also be stored in other facilities via techniques such as disk mirroring, provided the storage is secure in accordance with these requirements.

3.4.6.5 System Administration

The CCTV system must meet the logical security requirements in Appendix B.

3.4.7 Security Device Inspections

3.4.7.1 Semi-Annual Inspections

a) A semi-annual inspection must be conducted on all security devices and hardware including but not limited to:

- Alarm system
- Access-control system
- Window and door contacts

  - Glass-break detectors
  - Emergency door alarms
  - Passive infrared detectors
  - Microwave sensors
  - CCTV monitors
  - CCTV image recorders

b) Inspections must be carried out by an external organization qualified to perform such functions.

c) A copy of the inspection reports must be retained for at least 18 months.

3.4.7.2 Battery Testing

a) Batteries used in local alarms must be tested at minimum monthly and replaced annually (or in accordance with technical specifications provided by the supplier, if testing is more frequent).

b) Evidence (logs) must be retained for this testing for at least 18 months.

3.5 Vendor Security Contingency Plan

The vendor must have a written contingency plan to guarantee that security for card components, products, and data is maintained in case of critical business interruption.

3.6 Decommissioning Plan

a) The vendor must document its policies and procedures by which assets associated with card production and provisioning activities are secured in the event production activities are terminated.

b) The procedures must identify all data storage, card design materials, cards, card components, physical keys, cryptographic keys, and hardware utilized for production activities that must be secured.

c) The disposition expectations for each identified item must be defined. For example, items may be returned to the owner, transported to an authorized user, or destroyed.

4 Production Procedures and Audit Trails

4.1 Order Limitations

a) The vendor must only manufacture card products or components in response to a specific, signed order from a representative of the payment brand, issuer, or issuer's authorized agent.

b) The vendor must only produce sufficient cards to meet the quantity specified on the order.

c) If a function normally associated with card production or provisioning is subcontracted, the vendor must obtain authorization from the VPA and the issuer.

d) The information on the reverse of the cards must always identify the vendor that produces the card.

4.2 Card Design Approvals

4.2.1 Proof Submission

The vendor must follow submission procedures mandated by the appropriate payment brand to receive approval for the card design in order to confirm the design's compliance to the applicable payment brand standards.

4.2.2 Approval Response

The vendor must proceed with card manufacturing only after the submission has been approved.

4.3 Samples

4.3.1 Sample Retention

The vendor must maintain the following for each order:

a) All records of approval for the job from the applicable payment brand

b) A sample of the partially processed product or component

c) A portion of a printed sheet

d) Documentation indicating the source, quantities, and the distribution of each product received from an external company

e) All samples visually voided and functionally inoperable

4.3.2 Required Samples

When requested by the payment brand, the vendor must send samples of the finished cards or components from each production run before shipping the finished card products. These samples must be functionally inoperative, and it must be visibly apparent that they are not live cards.

4.4 Origination Materials and Printing Plates – Access and Inventory

a) The vendor must restrict access to the department or to the dark room where film, plates, or electronic media are produced or stored to authorized personnel.

b) Transfer of the printing films or printing plates and related responsibility from the pre-press staff to the card-printing staff must be documented in a specific audit sheet to be signed by the two persons involved on this transfer.

c) The audit sheet must contain at least the following:

- Signature of the pre-press staff delivering or collecting the printing films
- Job number identification and description of item(s) to be transferred
- Signature of the card printing staff collecting or delivering the printing films
- Quantity of item(s) transferred (number of films, front and reverse)
- Date and time of transfer

d) The vendor must inventory the films, printing plates, and duplicates including a record of plates issued from and returned to the printing department.

e) The vendor must audit this inventory quarterly.

f) The vendor must keep films and printing plates locked under dual control when not in use.

g) Materials maintained must be limited to the final approved version of the last production run of a particular card type.

h) After final use, films and printing plates must be voided or destroyed, and the log of destruction must be signed simultaneously by at least two persons in a specific destruction logbook.

i) All discrepancies must be documented and immediately reported to management. Any loss or theft of materials must be reported to the VPA within 24 hours of discovery.

4.5 Core Sheets and Partially Finished Cards

4.5.1 Core Sheets

4.5.1.1 Access

a) Access to unbundled core sheets must be restricted at all times.

b) Core sheets must be allocated for production use under a materials/production regimen.

4.5.1.2 Partially or Fully Printed Sheets

a) When partially or fully printed sheets are stored outside the vault for more than one week, they must be stored in a work-in-progress (WIP) storage room.

b) Audit or accountability forms for core sheets must provide the following information for every order processed:

- Good sheets
- Rejected sheets
- Set-up sheets

- Quality control sheets
- Unused core sheets

c) Sheets printed with the payment system brand or issuer design must not be used as set-up sheets unless clearly marked void over the payment-system brand/issuer design.

d) Once core sheets have been printed with a payment system brand mark, company logo, standard product design features, or an issuer design bearing the appropriate windows for the application of the logo, the printed sheet must become a part of the audit and accountability process. An accurate sheet count must be made and recorded in the initial count production control system.

e) If either side of a core sheet has been printed with what could be mistaken for payment system brand marks, card images or issuer designs, it must not be used as a set-up sheet on subsequent jobs, but instead be destroyed with other printed sheets that are unusable.

4.5.2 Partially Finished Cards

When partially finished cards (e.g., pre-personalized) are temporarily stored outside the vault, they must be stored in a secure, locked container in the HSA under dual control. Cards shall not be stored outside of the vault except as WIP while the facility is in operation

4.6 Ordering Proprietary Components

a) The vendor must obtain proprietary components (e.g., signature panels, holographic materials, special dies) only from authorized suppliers.

b) The vendor must provide the supplier with both the street and mailing addresses of the vendor’s facility, as well as names and signatures of the vendor’s authorized representatives that will be ordering components.

4.7 Audit Controls – Production

4.7.1 General

An order may be separated into multiple jobs, which may be split into different batches.

a) The vendor must apply audit controls to each job/batch received, whereby an effective audit trail is established for each production step.

b) All card products and components—both good and rejected, including samples—must be counted and reconciled prior to any transfer of responsibility.

c) An effective audit trail is comprised of a series of audit logs that must contain but are not limited to the following information:

  - Description of the component or card product(s) being transferred
  - Name and signature of the individual releasing the component or card product(s)
  - Name and signature of the individual receiving the component or card product(s)
  - Number of components or card products transferred
  - Number of components used
  - Number returned to vault or WIP storage
  - Number rejected or damaged
  - Number to be destroyed
  - Date and time of transfer
  - Name and signature of supervisor
  - Signatures of persons inventorying components

d) At the end of each production step, two persons must simultaneously count the card components and related components and sign the audit control documents.

e) Audit control documents must be completed and reconciled at the end of each production step and when changing shifts. They must be attached to or included with the work in process.

f) The vendor must be able to confirm that the material, including waste, used in the manufacture of card products matches the amount of material indicated in the inventory control logs. The audit trail must be kept for at least 24 months. This information must be available for inspection.

g) The vendor must maintain an original or a copy of both the purchase order and invoice for procured materials to serve as an audit control log.

h) The vendor must conduct inventory counts to ensure that invoices are correct and that they comply with the purchase order.

i) During the processing of card products (encoding, embossing, and personalizing), only the minimum number of boxes or sleeves required may be opened at one time. The contents of partially used boxes or sleeves must be verified against the inventory control documents. Before additional boxes or sleeves are opened, any partially used boxes or sleeves must be fully used. The number of cards in partially used boxes and sleeves must be verified, and each box or sleeve must be rewrapped and sealed before being stored in the vault.

j) Card components must be received and initially inventoried against the supplier's shipping documentation under dual control.

k) A physical count of the boxes containing the card components must be completed at delivery to confirm accuracy of the shipper's documents.

l) An authorized employee must sign for all component stock received by the vendor. The person delivering the stock must also sign the transfer document.

m) Card components must be transferred to the vault immediately.

n) The exact quantity of card components must be counted and registered in the inventory book before vault storage.

o) In the case of holograms, the hologram identification number to be registered as initial stock inventory must be the first good hologram image on the reel (this may be different from the number of holograms indicated in the delivery note).

p) The card component inventory log must include but is not limited to:

   - The reel number or equivalent control that provides unique identification.
   - Date of usage
   - Customer job number
   - Number of images or modules placed on cards
   - Number of rejected images or modules from header and trailer scrap
   - Number of and reason for rejected images

q) Card components must be removed from the machine and locked within a secure container when not in use.

r) Card components must be returned to the vault during non-production hours.

s) Rejected card components awaiting return for credits must be maintained under dual control.

4.7.1.1 Log Modifications

a) If modifications are to be made to the audit log, a single line must be made through the original figure.

b) The updated figure and the initials of the employee making the changes must be placed adjacent to the incorrect figure.

4.7.1.2 Log Review

All logs must be reviewed and validated for completeness at least weekly by an individual who is not involved in the direct operation of the equipment.

The review must be signed and dated as part of the log.

4.7.2 Vault Audit Controls

a) A log is required for items moved in or out of the vault and must contain:

   - Name of the card issuer
   - Type of card
   - Number of cards originally placed in inventory
   - Reason for transaction (e.g., job number)
   - Number of cards removed from inventory
   - Number of cards returned to inventory
   - Balance remaining in the vault
   - Date and time of activity
   - Names and signatures of the employees who handled the transaction

b) Two employees must create a written, physical inventory of card and card components monthly.

c) Employees performing the inventory must not have knowledge of the results of the last inventory.

d) At a minimum, the monthly inventory log must contain:

   - Date of the review
   - Name of the card issuer
   - Type of card
   - Number of cards indicated in the inventory
   - Number of cards counted
   - Name and signature of both employees who conducted the inventory

e) Any discrepancies must be reported to management and resolved.

4.7.3 Personalization Audit Controls

a) During personalization, cards and cardholder information must be handled in a secure manner to ensure accountability.

b) An audit control log must be maintained for each job/sub-job (batch) designating:

   - Job number
   - Issuer name
   - Card type

c) For each personalization batch, include:

   - Initial card procurement (beginning balance)
   - Card re-makes
   - Cards returned to inventory
   - Spoiled cards
   - Sample/test cards
   - Machine/operation identification
   - Date and time of reconciliation

- Operator name and signature
- Name and signature of an individual other than the operator, who is responsible for verifying the count

d) For accounts/envelopes, include:

- Number of accounts
- Number of card carriers printed
- Number of carriers wasted
- Number of envelopes that contain cards
- Operator name and signature
- Name and signature of an individual other than the operator, who is responsible for verifying the count

e) For PIN mailers, include:

- Number of mailers to be printed
- Number of mailers actually printed
- Wasted mailers that have been printed
- Number of mailers transferred to the mailing area/room
- Operator name and signature
- Name and signature of an individual other than the operator, who is responsible for verifying the count

4.8 Production Equipment and Card components

4.8.1 Personalization Equipment

The vendor must maintain a log of personalization equipment failures, including at a minimum:

a) Operator name

b) Supervisor name and signature

c) Machine description/number

d) Job number

e) Date

f) Time

g) Cause of the malfunction

4.8.2 Tipping Foil

a) The vendor must shred completely used tipping foil reels containing cardholder information as follows:

- In-house,
- Under dual control, and
- The destruction can occur as frequently as the vendor deems necessary but—in all cases—weekly at a minimum. The vendor must maintain proper controls over these materials at all times prior to destruction, and the destruction must occur within the HSA.

b) Used tipping foil must be removed from the machine during non-production hours

c) Prior to destruction—e.g., shredding—the foil must be stored within the HSA under dual access control.

d) When destroyed the results must be non-readable and non-recoverable

e) An inventory of the number of used reels must be maintained and reconciled with the number of reels shredded.

f) A log, pre-numbered and bound, of the destruction of the foil must be maintained and include at a minimum:

- Number of reels—partial or full. All used foil must be accounted for and destroyed.
- Date and time
- Written initials of both individuals who witnessed the destruction

4.8.3 Indent Printing Module

The vendor must:

a) Use payment system proprietary typefaces within indent-printing modules only for payment system cards.

b) Destroy, under dual control, payment system proprietary typefaces within indent-printing modules that are no longer to be used.

c) Record the destruction of modules.

4.9 Returned Cards/PIN Mailers

4.9.1 Receipt

The vendor must:

a) Maintain a log of all returned cards and PIN mailers.

b) Store all returned cards in a secure container under dual control.

c) Either send returned cards to the issuer or destroy them as defined in Section 4.10, “Destruction and Audit Procedures.”

d) Destroy returned PIN mailers as defined in Section 4.10 below.

e) Place cards collected by the vendor from a third-party location in a secure container under dual control before leaving the third-party location.

4.9.2 Accountability

a) The opening of the container and an accounting of the number of envelopes/cards must take place under dual control immediately upon receipt at the personalization facility.

b) The log must contain at a minimum:

- Date of receipt,
- Written initials of both employees counting the cards,
- The issuer name, and
- For each package:
  - i. The card type
  - ii. The number of envelopes
  - iii. The number of cards

4.10 Destruction and Audit Procedures

a) All waste components must be counted before being destroyed in-house and under dual control. A record of destruction by reel number and item count must be maintained for 24 months.

b) The following materials must be destroyed on a batch basis by shredding or grinding such that the resulting material cannot be reconstructed:

- Spoiled or waste card products
- Holographic materials
- Signature panels
- Sample and test cards
- Any other sensitive card component material or courier material related to any phase of the card production and personalization process.
- Destruction of chips, modules, or chip cards must ensure that the chip itself is destroyed.

c) An exception to the above is that holograms failing the hot-stamping process must be rendered unusable at the machine.

d) The material waiting to be destroyed must be stored securely, under dual control.

e) Destruction must be carried out in a separate room as defined in 3.3.5.3.

f) Proper destruction requires the following:

- Individuals destroying the materials must ensure that they are rendered unusable and unreadable.
- Two employees must simultaneously count and shred the material.
- Before leaving the room, both employees must ensure that all material has been destroyed and not displaced in the machinery or equipment.
- Employees must prepare, sign, and maintain a destruction document.
- Once the destruction process is initiated, the process must not be interrupted

g) An audit log must be created which, at a minimum, contains the following information:

- Signatures of the individuals presenting waste material
- Description of item(s) to be destroyed (such as product type, job number, and issuer name)
- Signatures of the persons observing or carrying out the waste destruction
- Quantity of item(s) to be destroyed
- Date and time of destruction

4.11 Lost and Stolen Reports

a) The vendor must immediately (within 24 hours) report to the VPA, the issuer, and appropriate law-enforcement agencies any loss or theft of card products or components.

b) The report must include but is not limited to:

- The complete and detailed chronology of events
- Cardholder account numbers
- Personal identification numbers (PINs)
- Printing plates
- Encoding or personalizing equipment
- Signature panels
- Holograms
- Electronic storage media
- Chips or any carrier containing card components
- The vendor's technical specification manual

c) The written communication must contain information regarding the loss or theft, including but not limited to the following:

- Name of issuer
- Type of card or product
- Name and address of the vendor
- Identification of source of cards
- Description of the incident including:
  1. i. Date and time of incident
  2. ii. Details of companies and persons involved
  3. iii. Details of the investigation
  4. iv. Name, e-mail address, and telephone number of the person reporting the loss or theft
  5. v. Name, e-mail address, and telephone number of the person to contact for additional information (if different from the person reporting the incident)

Additional or follow-up reports should be forwarded to the VPA, issuer, and the appropriate law-enforcement agencies as activities or actions occur.

5 Packaging and Delivery Requirements

Approved shipping methods are defined in the following table:

	Type of Delivery	Card Volume	Destination
Personalized Cards – Individual	Mail[1]	Individual Package	Cardholder
	Courier	Individual Package	Cardholder
		Unlimited	Issuer, an approved vendor, or (with written issuer and VPA consent) to another destination
	Secure Shipment	Unlimited	Issuer, an approved vendor, or (with written issuer[2] and VPA consent) to another destination
Personalized Cards – Bulk[2]	Mail	Not allowed	
	Courier	Unlimited	Issuer, an approved vendor, or (with written issuer[2] and VPA consent) to another destination
	Secure Shipment	Unlimited	Issuer, an approved vendor, or (with written issuer[2] and VPA consent) to another destination
Unpersonalized Cards – Bulk	Mail	Not allowed	
	Courier	Limited to 500/package/day/issuer/destination —e.g., branch	Issuer, an approved vendor, or (with written issuer[2] and VPA consent) to another destination
	Secure Shipment	Unlimited	Issuer, an approved vendor, or (with written issuer[2] and VPA consent) to another destination

[1] For transfer to the mail facility, personalized cards can be transported using a company vehicle with the following security controls:

- A GPS tracking device is used and monitored during transport from within the security control room.
- The contents are secured with tamper-evident straps and checked upon delivery.
- The vehicle is loaded using dual control and locked during transport.
- Vehicle drivers do not have a key or access to contents.
- Two persons are in the vehicle equipped with a device to communicate with the security control room

[2] This includes cards that have been personalized with a cardholder name, generic identifier, or no cardholder identifier.

1. If the vendor has subcontracted the manufacturing process to another approved vendor, the subcontracting vendor must assume responsibility during transportation for the loss/theft/misplacement of the cards and/or materials.
2. These shipments must be documented to include at least the following information:
   a) Name of the issuer
   b) Destination
   c) Date of shipment
   d) Name of courier
   e) Manifest number
3. The vendor must report to the VPA when a shipment request is not in compliance with these shipping requirements, and must withhold shipment until instruction from VPA is received.

5.1 Preparation

The vendor must:

a) Count all card products under dual control.
b) Complete audit-control documentation before the cards are packaged.
c) Reconcile all counts with amount to be shipped prior to packaging.
d) Immediately seal containers for final packaging.
e) Immediately investigate and resolve discrepancies.

5.2 Packaging

The vendor must:

a) Use materials for the packaging of cards and components with sufficient strength to minimize breakage during shipment.
b) Use packaging that does not indicate or imply the nature of the contents.
c) Use reinforced, tamper-evident, color-coded tape that is not in common use to band the containers.
d) Use containers that are uniquely numbered and labeled.
e) Record the number of containers and cards on a packing list.
f) Package all un-enveloped cards shipped in bulk in double-walled cartons that must have a bursting strength capable of handling a minimum 250 pounds (112 kgs) of pressure.
g) Each carton within a shipment must have the number of cards it contains printed on the carton, and the batch/shipment details of which it forms part.

5.3 Storage before Shipment

a) Card products awaiting shipment must be maintained under dual control in a vault when the facility is closed or in a HSA, where access is limited to authorized personnel only, when the facility is operational.

b) Packages that are opened or damaged must not be shipped until the contents are recounted and repackaged.

5.4 Delivery

PIN mailers and cards must be dispatched separately, a minimum of two days apart. The only exception is for the distribution of nonpersonalized prepaid cards, which may be distributed the same day in accordance with Section 6 of this document.

Electronic distribution of PINs may occur on the same day in accordance with the Logical Security Requirements – Section 10.

5.4.1 Mailing

a) Personalized cards must be placed in envelopes that are nondescript (e.g., envelopes must not contain any brand or other identifying marks) and the same size and color as other envelopes with which they may be presorted or delivered to the postal service.

b) After applying postage and sealing, the envelopes must be counted under dual control and placed in locked or sealed containers or bags.

c) A receipt of delivery must be signed by a representative of the receiving organization, and a signed copy of the receipt must be retained by the vendor.

5.4.1.1 Emergency Cards and PINs

Vendors may include the PIN with the mailing of emergency cards only with written approval from the issuer. Card vendors will be responsible for ensuring an appropriate officer of the card issuer has signed the authorization letter and that a copy of the letter is maintained in their files. The authorization letter must acknowledge that the issuer accepts all risk inherent in shipping cards and PINs together and must confirm that the expedited process is permitted only for emergency card replacement orders. Issuers may provide the card vendor with a standing letter of instruction and do not need to approve each emergency card replacement order.

5.4.1.2 Mail Trays (Awaiting Delivery to the Postal Service)

a) Mail must be in tamper-evident packaging, and/or strapped to prevent the removal of envelopes, or placed in locked carts.

b) The packaging must be the same as that used by the local mail service.

c) Package labeling must not indicate the name of the vendor or issuer.

d) If postal service mailbags are used in place of trays or locked carts, the bags must be sealed until transferred to the postal service.

e) The loading and transfer process must use the shipping and delivery areas as defined in Section 3.3.7, "Other Areas."

5.4.2 Courier Service

a) The vendor must secure packages under dual control with access limited to authorized personnel.

b) The vendor must only utilize a courier service that assigns a unique tracking number for each package. A tracking system in conjunction with the tracking number must enable the vendor to identify the successful completion of delivery milestones and exception conditions during the delivery process commencing with initial pick-up and ending with delivery.

c) The vendor must ensure packages sent by courier service contain a manifest prepared by the vendor that describes the package contents and enables content-verification upon receipt. The manifest prepared by the vendor must include but is not limited to:

- The type of each card
- The quantity per card type
- The job number(s)
- The date of shipment
- The date of receipt
- Name of receiving organization
- Name and signature of person receiving the cards

d) The contents of the manifest must be reconciled with the audit trail for the job.

e) Shipping of packages must not take place on the last working day of the week or the day before a public holiday unless the courier's operations and that of the recipient facilitate the delivery in the same manner as all other working days (i.e., they are both open for business).

f) Receipt of the shipment and count of contents must be confirmed by the recipient, immediately upon receipt under dual control.

5.4.3 Secure Transport

The vendor must confirm with the VPA whether specific requirements apply to its geographic locations.

There are four types of secure transport, as noted below:

5.4.3.1 Armored Vehicle

The contract with the carrier company must specify that**:**

a) This service must be carried out under dual control.

b) The card transport vehicle must not carry any signs or logos indicating it belongs to a card vendor.

c) If intermediate stops are made during transport, the carrier must ensure the integrity of the shipment remains intact. The cargo must never be left unattended unless the cargo area is armored.

d) If the cargo area is unarmored, the vehicle transporting the cards must be under dual control at all times (a driver accompanied by a guard) and never left unattended during the trip.

5.4.3.2 Unarmored Vehicle

Transport must occur in the following manner. If a carrier company is used, the contract must stipulate that:

a) An accompanying vehicle must be used. This vehicle must not also be used as a card transport vehicle.

b) The vehicle transporting the cards must be under dual control at all times (a driver accompanied by a guard) and never left unattended during the trip. The vehicle must be equipped with a telephone or have two-way radio contact with the security controller.

c) The card transport vehicle must not carry any signs or logos indicating it belong to a card vendor.

d) Deliveries must be direct (point to point), i.e., non-emergency stops are not permitted.

5.4.3.3 Air Freight

a) Goods must be secured in locked or sealed containers.

b) A nonstop transport between the vendor location and the destination location is required whenever possible.

c) A destination capable of handling secure cargo must be used.

d) If intermediate stops are made during air transport, the vendor must ensure the integrity of the shipment remains intact.

e) If any ground storage is required before, during, or after the flight, the location must be secured and inaccessible to unauthorized personnel.

f) Goods registered as consolidated cargo are not permitted.

g) The hand-carrying of goods is strictly prohibited.

5.4.3.4 Sea Freight

a) Goods must be secured in locked or sealed containers.

b) A nonstop transport between the vendor location and the destination location is required whenever possible.

c) The vendor must use container shipment.

d) The vendor must arrange delivery to and pick-up from dockside immediately.

e) Sea-freight service must be bonded.

f) Goods registered as consolidated cargo are not permitted.

g) The hand-carry of goods is strictly prohibited.

5.5 Shipping and Receiving

a) The vendor must not release card products or components unless the following minimum shipping requirements are met.

b) The vendor must:

- Have access to the names and signatures of individuals who are authorized to collect and deliver shipments.
- Verify the identity of personnel arriving to collect or deliver shipments.
- Confirm the identity with the signature list.

- Place the cartons on a pallet in such a manner that the sides of the carton showing the batch code are visible.
- Record the name and signature of individual collecting or delivering the shipment.

5.5.1 Procedures for Transportation and Receipt

The vendor must implement the following procedures:

a) Before release of the consignment, a pre-arranged method of identification between the vendor and destination party must be established to verify the authority and identity of the carrier to receive shipment.

b) At each point where custody and possession of the consignment changes from one entity or agent to another, the consignment must be inspected to confirm the integrity of all locks and seals.

c) A written receipt must be completed under dual control at each point of transfer, confirming the integrity of the consignment.

d) If there is evidence that a container has been tampered with, is missing, or is not received as scheduled at its final destination, the requirements for loss or theft of card products (Section 4.11) must be followed, and there must be no further movement of the shipment without notification to the issuer and VPA.

e) Obtain positive confirmation of receipt of shipment.

5.5.2 Receipt and Return of Card components

a) All card components must be delivered and returned by secure transport.

b) The consignment must be received under dual control.

c) Whilst under dual control, the consignment must be inventoried and handled as defined in ”Audit Controls” (Section 4.7).

d) Documentation of the shipment must be maintained for 24 months and must include:

   - Item description
   - Sequential identification numbers (if applicable)
   - Reel numbers
   - Total quantity returned
   - Recipient name and signatures
   - Destination or origination address
   - Shipping or receipt date and time

e) Prior to shipment, the vendor must ensure that the names and signatures of the authorized recipients are recorded.

i) At shipment, the vendor must verify the authorized signatures prior to transfer.

5.6 Establishing Responsibility for Loss

The transfer of shipment responsibility occurs at the point at which the vendor has delivered cards according to the contract between the issuer and the approved vendor.

6 PIN Printing and Packaging of Non-personalized Prepaid Cards

The following requirements apply only for non-personalized, prepaid cards. All other preceding requirements apply unless explicitly superseded in this section.

The PIN printing system may be a single, integrated device with multiple components (e.g., control system, HSM, and printer) or a system of separate components with dedicated functionality, connected via cables.

Prepaid cards may be packaged, shipped, and mailed together with their PINs, provided the following requirements are fulfilled:

1. The vendor must obtain written authorization from the issuer for packaging, shipping, or mailing the card and PIN together. This authorization must include confirmation that:
    a) Cards will not be activated or loaded with a stored value until they have reached their destination, and
    b) The issuer accepts all risk inherent in shipping or mailing cards and PINs together.
2. The vendor must ensure that an appropriate officer of the issuer has signed the authorization letter and must maintain a copy of the letter in its files until the card expiry date.
3. An employee who is involved in PIN printing must not be involved in the card personalization process or the packaging of the card with the PIN process. An audit trail must be created and maintained as evidence that this separation has been enforced.
4. The matching of a card with a pre-printed PIN mailer (e.g., affixing the card to a carrier on which the PIN has already been printed, or placing the PIN mailer and card into one package) must be performed in the personalization HSA or in a separate HSA that meets the physical and logical requirements for a personalization HSA.
5. Clear-text PINs must never be available on any system on the personalization network.
6. PIN printing systems must be either on a network physically separate from the personalization network or on a logically separated subnet dedicated for PIN printing, which is protected by a dedicated firewall.
7. Keys used for encrypting PINs must meet the key management requirements defined in the *PCI Card Production and Provisioning Logical Security Requirements* document.
8. PINs must be deleted from the PIN printing system immediately after printing using a secure erasure tool that prevents recovery of the PIN using forensic techniques or off-the-shelf recovery software.
9. The clear-text PIN must only be available for the minimum time required for printing and must not be stored.
10. If the clear-text PIN is available outside the printer at any time (e.g., in the memory of the controlling system or PC), the entire PIN printing system (including the HSM) must:
    a) Be in a dedicated PIN printing room as defined in the Section 3.3.5.4 of this document, "PIN Mailer Production Room"; and
    b) Only be made operational after physical review of the cabling has been performed and it is confirmed that there is no evidence of tampering.

    Additionally, the PIN must be concealed in tamper-evident packaging immediately after printing.

11. If the clear-text PIN is only available inside the single, integrated device (i.e., the HSM, controller, printer, and all cabling that carries the PIN are secured inside a single, integrated device), PIN printing may take place in any of the following places:

    a) The personalization HSA

    b) A dedicated PIN printing room within the personalization HSA

    c) A separate HSA that meets the physical and logical requirements for a personalization HSA

    d) Additionally, all of the following requirements must be fulfilled:

    e) The printer must be locked under dual control before the print job starts and any PINs are decrypted.

    f) The HSM in the printer must be under dual control at all times.

    g) The print job must only be started after a physical review of the chassis and cabling has been performed and it is confirmed that there is no evidence of tampering.

    h) The clear-text PIN must only be available inside a securely locked and covered area of the machine for the minimum time required for printing and must not be stored.

    i) The printed PIN must not be visible from outside the machine at any time—i.e., the machine must be covered to prevent observation and the covers must be locked in place with dual control locks.

    j) The PIN must be concealed in tamper-evident packaging immediately after printing and before leaving the secured confines of the printer.

Appendix A: Applicability of Requirements

Physical Security Requirements				
Requirement	Physical Cards	Mobile Provisioning		Conditions
		SE	HCE	
Section 2 - Personnel				
All	X	X	X	All requirements applicable
Section 3 – Premises				
All	X	X	X	All requirements applicable
Section 4 – Production Procedures and Audit Trails				
4.1	X	X	X	Only 4.1c applies for mobile provisioning
4.2	X			
4.3	X			
4.4	X			
4.5	X			
4.6	X			
4.7	X			
4.8	X			
4.9	X			
4.10	X			
4.11	X			
Section 5 – Packaging and Delivery Requirements				
All	X			All requirements applicable
Section 6 – PIN Printing and Packaging of Non-personalized Prepaid Cards				
All	X			All requirements applicable

Appendix B: Logical Security Requirements – CCTV and Access Control System Administration

All system components and software must be managed in accordance with the following except for purpose-built appliances such as digital video recorders (DVRs). Purpose-built appliances and similar devices are generally not susceptible to malware and other vulnerabilities and frequently do not support anti-virus and/or patching. Any appliance based on an operating system such as Linux or Windows must be isolated from other networks and not use open connectivity methodologies, such as IP.

All systems commonly impacted by malicious software and similar vulnerabilities, such as personal computers and servers, must meet these criteria. Additionally, all user management, including password controls, must be implemented except where the platform does not support that degree of granularity. Regardless, controls must be implemented to the degree possible.

B.1 User Management

The vendor must:

a) Ensure that procedures are documented and followed by security personnel responsible for granting access to the CCTV and access control systems

b) Restrict approval and level of access to staff with a documented business need before access is granted. At a minimum, documented approvals must be retained while the account is active.

c) Restrict systems access by unique user ID to only those individuals who have a business need.

d) Only grant individuals the minimum level of access sufficient to perform their duties.

e) Make certain that systems authentication requires at least the use of a unique ID and password.

f) Restrict administrative access to the minimum number of individuals required for management of the system.

g) Ensure security guards do not have administrative access.

h) Prevent remote administrative access from outside the facility

i) Ensure that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values.

j) Ensure that where generic administrative accounts cannot be disabled, these accounts are used only when unique administrator sign-on credentials are not possible and only in an emergency.

k) Ensure that when generic administrative accounts are used, the password is managed under dual control where no individual has access to the full password. Each component of the password must comply with the password control requirements in the next section.

l) Validate all system access at least quarterly.

m) Revalidate employee access to any systems upon a change of duties.

n) Ensure that access controls enforce segregation of duties.

o) Strictly limit privileged or administrative access and ensure such access is approved by both the user's manager and the security manager.

p) Establish management oversight of privileged access to ensure compliance with segregation of duties.

q) Ensure that all privileged administrative access is logged and reviewed weekly.

B.2 Password Control

B.2.1 General

The vendor must:

a) Implement a policy and detailed procedures relating to the generation, use, renewal, and distribution of passwords.

b) Implement procedures for handling lost, forgotten and compromised passwords.

c) Distribute password procedures and policies to all users who have access to cardholder information or any system used as part of the personalization process.

d) Ensure that only users with administrative privileges can administer other users' passwords.

e) Not store passwords in clear text.

f) Change all default passwords.

B.2.2 Characteristics and Usage

The vendor must ensure that:

a) Systems are configured so that newly issued and reset passwords are set to a unique value for each user.

b) Newly issued passwords are changed on first use.

c) "First use" passwords expire if not used within 24 hours of distribution.

d) Systems enforce password lengths of at least eight characters.

e) Passwords consist of a combination of at least three of the following:

   i. Upper-case letters

   ii. Lower-case letters

   iii. Numbers

   iv. Special characters

f) Passwords are not the same as the user ID.

g) Passwords are not displayed during entry.

h) Passwords are encrypted during transmission and rendered unreadable when stored.

i) Passwords have a maximum life not to exceed 90 days and a minimum life of at least one day.

j) When updating passwords, the system prevents users from using a password that is the same as one of their previous four passwords.

k) The user's identity is verified prior to resetting a user password.

l) Authentication credentials to the tokenization process are secured to prevent unauthorized disclosure and use.

B.3 Session Locking

The vendor must enforce the locking of an inactive session within a maximum of 15 minutes. If the system does not permit session locking, the user must be logged off after the period of inactivity.

B.4 Account Locking

a) Accounts that have been inactive for a specified period (with a maximum of 90 days) must be removed from the system.

b) Systems must enforce the locking of a user account after a maximum of six unsuccessful authentication attempts.

c) Locked accounts must only be unlocked by the security administrator. Alternatively, user accounts may be unlocked via automated password reset mechanisms. Challenge questions with answers that only the individual user would know must be used. These questions must be designed such that the answers are not information that is available elsewhere in the organization, such as in the Human Resources Department.

d) A user's account must be locked immediately upon that user leaving the vendor's employment until it is removed.

e) A user's account must be locked immediately if that user's password is known or suspected of being compromised.

f) The user account logs including but not limited to the following must be reviewed at least twice each month for suspect lock-out activity:

B.5 Anti-virus software or programs

The vendor must:

a) Define, document, and follow procedures to demonstrate:

- Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT)
- Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components
- Inventory of current systems in the environment including information about installed software components and about running services

b) Deploy anti-virus software on all systems potentially affected by malicious software—e.g., personal computers and servers.

c) Ensure that all anti-virus programs detect, remove, and protect against all known types of malicious software.

d) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

e) Check for anti-virus updates at least daily, and install updates in a manner consistent with Patch Management. Documentation must exist for why any updates were not installed.

B.6 Configuration and Patch Management

The vendor must:

a) Implement a documented procedure to determine whether applicable patches and updates have become available.

b) Make certain a process is implemented to identify and evaluate newly discovered security vulnerabilities and security patches from software vendors.

c) Ensure that secure configuration standards are established for all system components.

d) Ensure that the configuration standards include system hardening by removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

e) Ensure that the configuration of all system components associated with data transmission, storage, and personalization are validated against the authorized configuration monthly.

f) Evaluate and install the latest security-relevant patches for all system components within 30 days of their release (if they pass validation tests).

g) Verify the integrity and quality of the patches before application, including source authenticity.

h) Make a backup of the system being changed before applying any patches.

i) Implement critical patches to all Internet-facing system components within 7 business days of release. When this is not possible the CISO, security manager, and IT director must clearly record that they understand that a critical patch is required and authorize its implementation within a maximum of 30 business days.

j) Ensure that emergency hardware and software implementations comply with the procedures and validation requirements established for emergency implementations.

k) Ensure that emergency hardware and software implementations follow the configuration and patch management requirements in this section.

B.7 Audit Logs

The vendor must:

a) Ensure that audit logs exist for the CCTV and access control systems This includes operating system logs, security software logs or product logs and application logs containing security events.

b) Ensure that audit logs include at least the following components:

   i. User identification

   ii. Type of event

   iii. Valid date and time stamp

   iv. Success or failure indication

   v. Origination of the event

   vi. Identity or name of the affected data, system component, or resources

   vii. Access to audit logs

   viii. Changes in access privileges

c) Ensure that procedures are documented and followed for audit log review and reporting of unusual activity. Log reviews may be automated or manual and must occur at least monthly.

d) Verify at least once a month that all systems are meeting log requirements.

e) Ensure that logs are backed up daily, secured, and retained for at least one year. Logs must be accessible for at least three months online and one year offline.

f) Protect and maintain the integrity of the audit logs from any form of modification.

g) Implement a security-incident and event-logging framework for its organization.

Glossary

Term	Definition
Anti-pass-back	A security mechanism preventing an access card or similar device from being used to enter an area a second time without first leaving it (so that the card cannot be passed back to a second person who wants to enter).
Area	Area is an unenclosed space, with the exception of the HSA.
Armored Vehicle	The armored vehicle is designed to protect and ensure the well-being of the transported individuals. These vehicles are designed to resist attempts at robbery or hijacking through the use of bullet-resistant glass and reinforced shell/cab to protect occupants. If the cargo area itself is not armored, additional stipulations apply.
Authorized Personnel	Employees who have been authorized by the security manager or other executive to undertake specific roles or functions
Card Components	This includes sensitive materials such as, but not limited to a) Holographic materials b) Origination materials c) Signature panels d) Core sheets or cards printed with the brand mark e) Chips f) Materials containing any of the above
Cardholder Data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.
Card Manufacturer	An entity that is responsible for producing cards on behalf of a card issuer. The set of services performed depends on its contractual relationship with the issuer and may include part, or all, of the card production process.
Card Manufacturing	Card production process composed of the following phases: a) Pre-press (card design layout, printing films, and printing plates generation) b) White-plastic sheets printing c) Sheets assembly d) Sheets lamination e) Sheets cutting or punching f) Hologram and signature panel hot stamping
Card Products	Cards and the components required to manufacture a credit or debit card, such as plastic sheets, chips, contact plates, etc.
Chip	The integrated circuit that is embedded into a plastic card designed to perform processing or memory functions. See also *Chip Card.*

Term	Definition
Chip card	A card or device embedded with an integrated circuit or chip that communicates information to a point-of-transaction terminal. Chip cards offer increased functionality through the combination of significant computing power and substantial data storage.
Chip Embedding	The process by which an integrated circuit is permanently attached to the plastic of a payment card to become an integral part of that card.
Chip Personalization	Any process that writes issuer- or cardholder-specific data to the integrated circuit on the card. Generally includes: a) Bank branch identification (optional) b) Cardholder account number c) Cardholder name d) Validity dates e) Company identification (optional)
CISO	Chief Information Security Officer. Senior-level executive within an organization responsible for establishing and maintaining programs to ensure information assets are adequately protected.
Cloud-Based Provisioning	Preparation and delivery of Host Card Emulation data to a device
COTS	Commercial off-the-shelf (consumer-grade) devices such as mobile phones and tablets.
Data Preparation	Any formatting, sorting, or other manipulation of personalization data in readiness for card production.
Dual Presence	Two or more individuals are in the HSA as a whole. This does not supplant or replace any requirements for dual control. For example if three people are in the HSA, and two go into a room that requires dual control, the requirement for dual presence in the HSA as a whole is still met.
Encoding	Process by which data is written to the magnetic stripe located on the card.
Embossing	Personalization process that produces raised characters on the plastic card body. Embossing requirements may vary by card program, but generally include: a) Cardholder account number b) Cardholder name c) Validity dates d) Company identification (optional) e) Payment brand security characters
Goods-Tools Trap	Controlled area for transfer of materials between two areas.
High Security Areas (HSAs)	Areas in production facilities where card products, components, or data associated with personalization or mobile provisioning is stored or processed.

Term	Definition
Host Card Emulation (HCE)	Technology that permits a device to perform the function of a payment card on a Near Field Communication (NFC)-enabled device or via In-Apps without the use of a secure element.
HSA Rooms	HSA rooms are enclosed spaces with controlled access in production facilities where card products, components, or data are stored or processed, and are where card-production activities occur.
Indent Printing Module	Component of the personalization equipment that can be used to print account number and card validation code on the back of a card. These values are printed using a reverse italic font, which creates a physical indent on the card as per payment system specifications. This component is usually a separate module that is removable and can be replaced. When used by a payment system, the indent-printing module is a security feature that is sensitive and must be protected while in the vendor's possession.
Issuer	An entity licensed by a payment brand to issue cards and enter into a contractual relationship with the cardholder.
Mobile Provisioning	The personalization (provisioning) of a commercial off-the-shelf (COTS) device, such as an NFC-equipped mobile phone with appropriate cardholder account information. The information is transmitted to the device by a process called over-the-air (OTA) provisioning or, alternatively, over-the-internet (OTI).
Non-Personalized Cards	Cards that have been through the personalization process and have account data embossed or printed on the card and/or chip and magnetic stripe according to the scheme's rules but are not associated with a cardholder.
OTA	Over-the-air (OTA) refers to any process that involves the transfer of data (including applications) to the mobile device or any component within the mobile device via a mobile network.
OTI	Over-the-Internet (OTI) A remote connection from a security domain in the secure element to a backend server, using TLS over HTTP.
Personalization	The process of applying the account and, when required for the product, cardholder-specific data to the card, uniquely tying the card to a given account. This includes encoding the magnetic stripe, embossing the card (if applicable), and loading data on to the chip. Personalization uses technology such as: a) Embossing b) Laser engraving c) Thermal transfer d) Indent printing
Personalized Cards	Cards that have been through the personalization process and are associated with an individual person. That person's name may be encoded, embossed, or printed on the card and/or chip and magnetic stripe according to the scheme's rules.
Pre-personalization (Chip Initialization)	The process of replacing a transport key on a chip with an issuer-specific key and (optionally) activating the application.

Term	Definition
Secure or Sensitive Job or Task	Jobs and tasks in association with card production or provisioning.
Secure Element	Tamper-resistant module in a mobile device capable of hosting/embedding applications in a secure manner. A secure element may be an integral part of the mobile device or may be a removable element that is inserted into the mobile device for use.
Security Components	Security features that protect the card and may vary from payment brand to payment brand—e.g., holographic materials, signature panels, indent-printing modules when not installed.
Security Manager	Manager designated with the overall responsibility for physical security for the card production and provisioning facility. The Security Manager must not report to the production manager or director. There must also be a nominated Deputy Security Manager to cover when the Security manager is not on site.
Segregation of Duties	Practice of dividing steps in a function among different individuals so as to keep a single individual from being able to subvert the process.
Unpersonalized Cards	Cards that have not been through a personalization process, are not unique, and have no cardholder or account data on them.
Vendor	The legal entity and its associated premises that undertakes card production or provisioning.
Vendor Agent	A vendor agent is a separate organization or legal entity from the certified vendor that performs sales or promotional activities on behalf of a certified vendor. The agent is not authorized to physically take possession of a card or perform any card production or provisioning activities for which certification is required. Actual card production, provisioning and distribution services are performed by the certified vendor at an authorized facility.
Vendor Program Administrator (VPA)	The payment system contact person or team that manages vendor compliance with the security requirements defined in this document.