Payment Card Industry (PCI)

Card Production and Provisioning Security Requirements

Summary of Changes from PCI Card Production and Provisioning Version 2.0 to 3.01

September 2022

Table of Contents

Introduction

This document provides a summary of changes from *PCI Card Production Physical Security Requirements* and *PCI Card Production Logical Security Requirements* Version 2.0 to Version 3.0. The table below provides an overview of the types of changes included in Version 3.0. Sections 1 and 2 on the following pages provide summaries of material changes to be found in both the Physical and Logical Security Requirements documents.

Change Types

Change Type	Definition
Additional Guidance	Explanation, definition, and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Requirement Change	To reflect the addition or modification or deletion of requirements.

Note: *The changes above do not include those that are corrections of grammar or typographical errors or other rephrasing of existing statements.*

Section 1: Summary of Changes to Physical Security Requirements

Reference	Change to Physical Security Requirements	Type
General	Added Test Procedures to document.	Additional Guidance
General	Renumbered requirements from 2 through 6 to 1 through 5.	Additional Guidance
General	Replaced term, “employee,” throughout document with “personnel,” “individual,” “card production staff,” or “consultant” as applicable.	Additional Guidance
General	Changed badge system to access-control system throughout.	Requirement Change
Requirement 1 – Roles and Responsibilities		
1.1.1 Vendor Roles	Defined roles that must be filled by employees of vendor.	Requirement Change
1.1.6 Security Communication and Training	Clarified that information concerning security at vendor facilities can be done via posters, notices, or electronic medium.	Requirement Change
1.2.1.1 Prescreening	Allow that, for contracted guards, evidence of prescreening requirements may alternatively be provided by the guarding company, by copies of licenses, etc.; however, the vendor must collect and retain this evidence. Allow that vendors may use their own insurance policies to provide suitable liability coverage for contracted guard services.	Requirement Change
1.2.1.2 Restrictions/Limitations	Added conditions under which personnel pre-designated by management as first responders can enter the HSA.	Requirement Change
1.2.2 Roles and Responsibilities	Clarified responses for unauthorized access attempts using language from previously published FAQ.	Requirement Change
Requirement 2 – Premises		
2.1.3 External Walls, Doors, and Windows	Specified criteria for openings in external wall and that HSA windows must be non-openable.	Requirement Change

Reference	Change to Physical Security Requirements	Type
2.3.2.1 Location and Security Protection	Specified that Security Control Room windows must be non-openable.	Requirement Change
2.3.4.1 Access Control	Allow for use of audible alarms. Specified that access-control server must be located in the same facility.	Requirement Change
2.3.4.3 Transfer of Physical Materials	Added shipping and delivery area to good-tools trap and redefined as a requirement regarding transfer of materials between different HSAs within the same facility. Clarified that the above applies to physical materials.	Requirement Change
2.3.4.4 Security Controls	Clarified that the requirement for bullet-resistant glass or iron bars applies to windows on the exterior wall or door of the building.	Requirement Change
2.3.5.6 Vault	Added *EN 1143-1 Secure storage units - Requirements, classification, and methods of test for resistance to burglary - Part 1: Safes, ATM safes, strongroom doors, and strongrooms: Grade 6 or higher* may be used as equivalent to UL 608 Class1 Burglary Certification.	Requirement Change
2.3.6.2 Shipping and Delivery Areas	Changed log retention from permanent to two years where it is necessary to liberate a person inside the room.	Requirement Change
2.3.6.2 Shipping and Delivery Areas	Clarified outer room requirements for existing vs. new facilities.	Additional Guidance
2.4.1 Alarm Systems	Clarified that codes must be deactivated upon termination of any card production staff with knowledge of the code, and that only guards and security team members should have such knowledge.	Requirement Change
2.4.2 Badge Administration	Modified badge to access-control system throughout.	Requirement Change
2.4.2.1 Identification Badges	Modified to include lanyards.	Requirement Change
2.4.3 Badge-Access System	Stipulate that for multiple buildings within the same facility, a single central location for a badge-access system can administer all buildings and the conditions for use of a public or private network.	Requirement Change

Reference	Change to Physical Security Requirements	Type
2.4.3.3 Remote-access Controls	New section using pre-existing requirements.	Additional Guidance
2.4.7.1 Semi-Annual Inspections	Specified that testing must also occur in addition to inspection for all security devices and hardware.	Requirement Change
2.4.7.2 Battery Testing	Clarified battery testing criteria.	Requirement Change
Requirement 3 – Production Procedures and Audit Trails		
3.7.1.2 Log Review	Specified that all logs in this document must be retained for a minimum of two years unless otherwise stated.	Requirement Change
3.8.4 Thermal Transfer Foil	Added section to address thermal ribbon.	Requirement Change
Requirement 4 – Packaging and Delivery Requirements		
4	Modified stipulations for courier delivery. Updated Terminology for consistency. Clarified that sample cards or proofs sent to an issuer or payment brand are out of scope for this requirement.	Requirement Change
4.3 Packaging	Clarified package bursting strength language.	Requirement Change
4.5 Delivery Requirements	Specified additional criteria.	Requirement Change
4.5.1 Card Mailing	Clarified envelope criteria and use of presort facilities. Added criteria for transfer to the mail facility.	Requirement Change
4.5.1.2 Mail Trays (Awaiting Delivery)	Clarified package labelling requirement.	Requirement Change
4.5.2 Courier Service	Specified additional criteria for unpersonalized bulk cards.	Requirement Change
4.5.3.1 Unarmored Vehicle	Aligned language with additions added to Air and Sea Freight.	Requirement Change
4.5.3.3 Air Freight	Added transport requirements for to and from air terminal.	Requirement Change

Reference	Change to Physical Security Requirements	Type
4.5.3.4 Sea Freight	Added transport requirements for to and from the port facility.	Requirement Change
4.5.3.5 Rail Freight	Added new section for Rail Freight.	Requirement Change
Appendix B: Logical Security Requirements – CCTV and Access-Control System (ACS) Administration		
B.1 User Management	Specified minimum capabilities for CCTV and access-control system upgrades. Clarified remote administrative access exception if used in conjunction with an approved SOC. Added password length requirement exception where system does not support.	Requirement Change
B.2.2 Characteristics and Usage	Systems enforce password lengths of at least 12 characters or an equivalent strength.	Requirement Change
Appendix C		
Appendix C	New Section, “Security Operations Center”	Requirement Change
Glossary		
Glossary	Added glossary definitions for: Card Production Staff, Dual Control, Facility, Participating Payment Brand and Public Network.	Additional Guidance

Section 2: Summary of Changes to Logical Security Requirements

Reference	Change to Logical Security Requirements	Type
General	Added Test Procedures to document.	Additional Guidance
General	Renumbered requirements from 2 through 10 to 1 through 9.	Additional Guidance
General	Replaced term “employee” throughout document with “personnel” or “card production staff” as applicable.	Additional Guidance
General	Added FIPS 140-3 to wherever 140-2 is required.	Requirement Change
General	Changed badge system to access-control system throughout.	Requirement Change
Requirement 1 – Roles and Responsibilities		
1.2 Assignment of Security Duties	Specified that the back-up CISO and the IT Security Manager must be employees of the vendor.	Requirement Change
Requirement 2 – Security Policy and Procedures		
2.1 Information Security Policy	Clarified that the information security policy must be disseminated to all relevant personnel (including vendors and business partners).	Requirement Change
Requirement 3 – Data Security		
3.4 Transmission of Cardholder Data	Clarified that preauthorized sources are defined and documented.	Requirement Change
Requirement 4 – Network Security		
4.2 General Requirements	Clarified that diagrams for the flow of cardholder and cloud-based provisioning data within the environment from its receipt/generation to end of its lifecycle must be kept current. Added that diagrams of the flow of cardholder and cloud-based provisioning data within the environment from its receipt/generation to end of its lifecycle must be reviewed for accuracy at least every 12 months.	Requirement Change

Reference	Change to Logical Security Requirements	Type
4.6.1 Connection Conditions	Clarified access from outside the facility to the badge physical access-control system exception if used in conjunction with an approved SOC.	Requirement Change
4.8.2 Penetration	Clarified the use of Common Vulnerability Scoring.	Requirement Change
Requirement 6 – User Management and System Access Control		
6.1 User Management	Added additional criteria for multi-factor authentication. Added password length requirement exception where system does not support.	Requirement Change
6.2.2 Characteristics and Usage	Changed to requiring 12-character password minimums from 8 characters. Exception if the operating system does not support twelve characters then using the maximum the system supports, but never less than a minimum length of eight characters.	Requirement Change
Requirement 7 – Key Management: Secret Data		
7.4.2 Key Manager	Specified that deputy key manager must be an employee.	Requirement Change
7.7 Key Loading	Clarified roles of key custodians and key manager for key loading.	Requirement Change
Requirement 9 – PIN Distribution via Electronic Methods		
8.1 General Principles	Added criteria for generating keys and key components using a random or pseudo-random process.	Requirement Change
Normative Annex A		
Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms	Updated consistent with other standards. Added EdDSA as an approved algorithm.	Additional Guidance

Reference	Change to Logical Security Requirements	Type
Glossary of Acronyms and Terms		
Glossary of Acronyms and Terms	Added glossary definitions for: Card Production Staff, Facility, Media, Multi-factor authentication, Non-console Access, Participating Payment Brand, Private Network, Public Network, and Topology Diagram; and clarified Remote Access.	Additional Guidance