Payment Card Industry (PCI)
Secure Software Standard

Sensitive Asset Identification
For use with the PCI Secure Software Standard v2.x

January 2026

Document Changes

Date	Version	Description
January 2026	1.0	Initial publication for use with the PCI Secure Software Standard v2.x.

Contents

Introduction

This document **is required** to be used in conjunction with the *PCI SSF - Secure Software Standard v2.x* (“Secure Software Standard,” or “the/this standard”).

Appendix A in this document is an optional section that contains tables to help the software vendor capture necessary information regarding sensitive assets. The software vendor can extract the tables/pages in Appendix A and add rows as needed to document the required information that will be used as part of the software assessment.

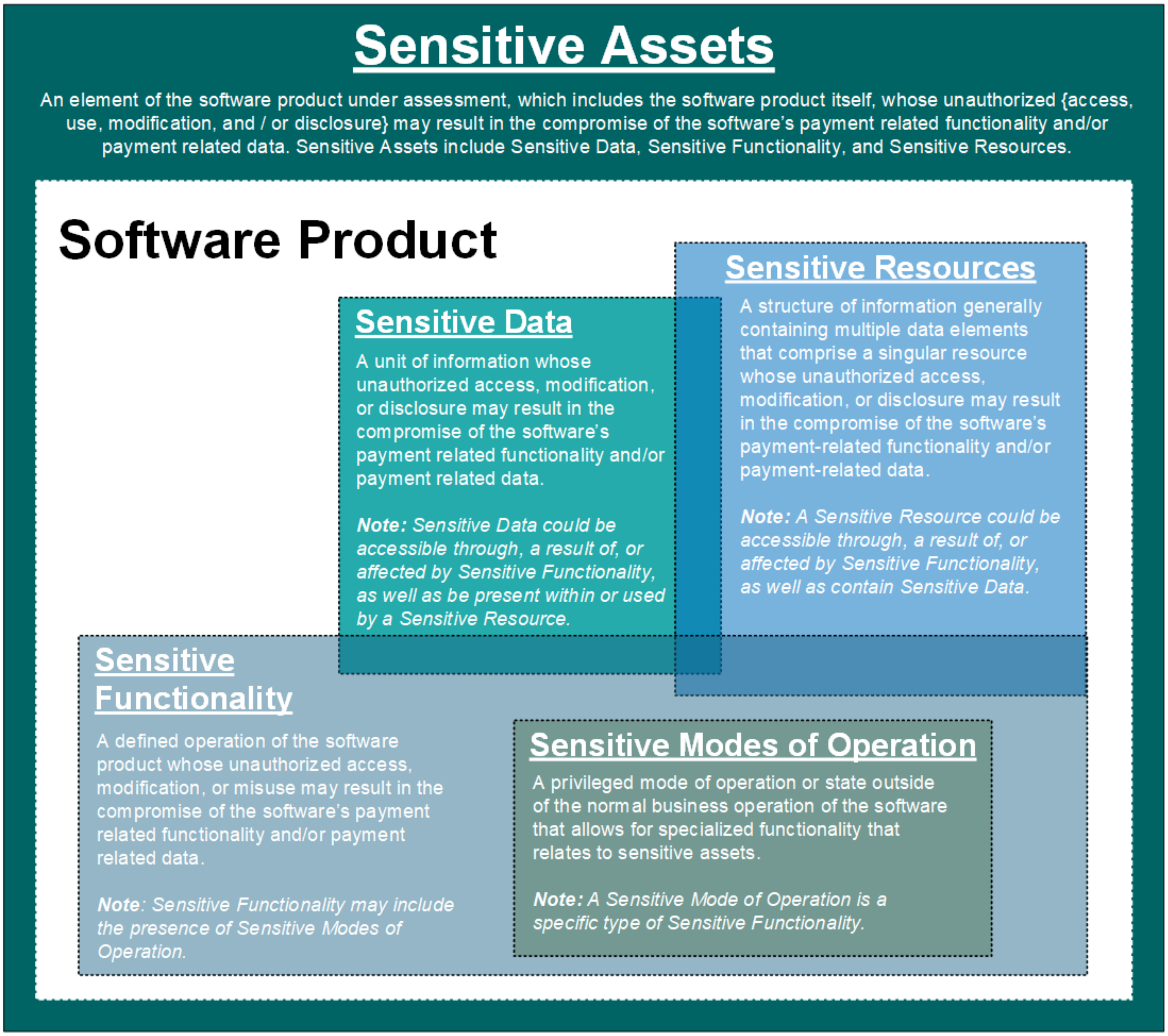
Do NOT modify or otherwise delete any information within this document.

Sensitive Assets

The *PCI Secure Software Standard* establishes security objectives and associated security requirements for the purpose of protecting sensitive assets related to the software’s payment-related functionality and/or payment-related data. The following definitions are imperative to this standard. Refer to the additional tables in this document for categories and examples of these definitions.

Sensitive Asset	An element of the software product under assessment, which includes the software product itself, whose unauthorized access, use, modification, and/or disclosure may result in the compromise of the software’s payment-related functionality and/or payment-related data. ***Note***: *Sensitive Assets include Sensitive Data, Sensitive Functionality, and Sensitive Resources.*
Sensitive Data	A unit of information whose unauthorized access, modification, or disclosure may result in the compromise of the software’s payment-related functionality and/or payment-related data. ***Note***: *Sensitive Data is a type of Sensitive Asset. Sensitive Data could be accessible through, a result of, or affected by Sensitive Functionality, as well as be present within or used by a Sensitive Resource.*
Sensitive Resource	A structure of information, generally containing multiple data elements that comprise a singular resource, whose unauthorized access, modification, or disclosure may result in the compromise of the software’s payment-related functionality and/or payment-related data. ***Note***: *A Sensitive Resource is a type of Sensitive Asset. A Sensitive Resource could contain Sensitive Data. A Sensitive Resource could be accessible through, a result of, or affected by Sensitive Functionality.*
Sensitive Functionality	A defined operation of the software product whose unauthorized access, modification, or misuse may result in the compromise of the software’s payment-related functionality and/or payment-related data. ***Note***: *Sensitive Functionality is a type of Sensitive Asset. Sensitive Functionality could include the presence of Sensitive Modes of Operation.*
Sensitive Mode of Operation	A privileged mode of operation or state outside of the normal business operation of the software that allows for specialized functionality that relates to sensitive assets. ***Note***: *A Sensitive Mode of Operation is a specific type of Sensitive Functionality.*

Figure 1: Sensitive Assets



Sensitive Assets

An element of the software product under assessment, which includes the software product itself, whose unauthorized {access, use, modification, and / or disclosure} may result in the compromise of the software's payment related functionality and/or payment related data. Sensitive Assets include Sensitive Data, Sensitive Functionality, and Sensitive Resources.

Software Product

Sensitive Data

A unit of information whose unauthorized access, modification, or disclosure may result in the compromise of the software's payment related functionality and/or payment related data.

Note: *Sensitive Data could be accessible through, a result of, or affected by Sensitive Functionality, as well as be present within or used by a Sensitive Resource.*

Sensitive Resources

A structure of information generally containing multiple data elements that comprise a singular resource whose unauthorized access, modification, or disclosure may result in the compromise of the software's payment-related functionality and/or payment-related data.

Note: *A Sensitive Resource could be accessible through, a result of, or affected by Sensitive Functionality, as well as contain Sensitive Data.*

Sensitive Functionality

A defined operation of the software product whose unauthorized access, modification, or misuse may result in the compromise of the software's payment related functionality and/or payment related data.

Note*: Sensitive Functionality may include the presence of Sensitive Modes of Operation.*

Sensitive Modes of Operation

A privileged mode of operation or state outside of the normal business operation of the software that allows for specialized functionality that relates to sensitive assets.

Note: *A Sensitive Mode of Operation is a specific type of Sensitive Functionality.*

The security objectives and security requirements of the standard are designed to facilitate the protection of sensitive assets from unauthorized access, disclosure, modification, and/or misuse, as appropriate.

The specific sensitive assets used in a software product are expected to be unique to how that software operates. Therefore, a comprehensive list is required to be developed as part of the evaluation of the software product to the standard, with cooperation between the software product vendor and the software assessor.

The software vendor is expected to account for any additional sensitive assets not denoted herein that are present within, or are an element of, the software product. The software vendor can also regard any additional assets as being sensitive to include them in the scope of their software assessment.

Sensitive Asset Protection Categories

The following table provides the protection categories and descriptions.

Table 1: Protection Categories

Protection Category	Purpose
Confidentiality (C)	Ensuring information is not made available or disclosed to unauthorized individuals, entities, processes, or comparable.
Integrity (I)	Ensuring the consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction.
Integrity with the addition of authentication (I+)	Ensuring the integrity of the data in addition to verifying the identity of individuals, entities, processes, or comparable attempting to access the data.

Sensitive Data Categories

The following table is intended to be used as a guide to assist in identifying the sensitive data that could be present in the software. This table is not exhaustive.

The defining factor of sensitive data is its definition. Therefore, qualifying sensitive data requires understanding both the type and use of the data element within the software.

Software vendors need to conduct a thorough review of the data stored, processed, and/or transmitted by the software to identify all forms of sensitive data that require protection, and implement security controls (including those defined within the standard) as appropriate to protect such information. Software vendors and software assessors work together to validate the sensitive data of the software and the protection mechanisms employed.

Table 2: Sensitive Data Categories

Sensitive Data Categories	Description	Minimum Required Protection Type
Account Data	Account Data consists of cardholder data (CHD) and/or sensitive authentication data (SAD). Refer to the “Account Data” section in this document for additional information.	In accordance with the latest *PCI DSS*
Attestation Data	Data that is used to determine, or confirm, the security or integrity of the software and/or its operational environment (e.g., that the software is behaving as expected, is properly configured, or is operating in a secure state). E.g., data collected on a client-side system that is sent to a back-end or server-side system.	C & I+
Authentication Data	Elements used to securely authenticate users, services, files, parameters, software, etc. E.g., passwords, tokens, cryptographic signatures, etc. ***Note****: This does NOT include “Sensitive Authentication Data (SAD).”*	Depends on the type and use
Cardholder Data (CHD)	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.	In accordance with the latest *PCI DSS*

Sensitive Data Categories	Description	Minimum Required Protection Type
Cryptographic Material associated with Sensitive Assets	All materials involved in the implementation of a cryptographic algorithm or process. E.g., entropy seeds, nonces, IVs, salt, random numbers, key components, etc.	C & I
EMV® 3DS related Data	Refer to the “EMV® 3-D Secure” section in this document.	
Primary Account Number (PAN)	Unique payment card number that identifies the issuer and the cardholder account.	In accordance with the latest *PCI DSS*
Public Keys	Cryptographic keys that are used to protect other sensitive assets and/or used by sensitive functionality. E.g., RSA public key	I
Secret/Private Keys	Cryptographic keys that are used to protect other sensitive assets and/or used by sensitive functionality. E.g., KEKs, DEKs, BDKs, LMKs, Private Keys, etc.	C
Sensitive Authentication Data (SAD)	Security-related information used to authenticate cardholders and/or authorize payment card transactions. This information includes, but is not limited to, card verification codes, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.	In accordance with the latest *PCI DSS*
This table is not exhaustive. **The examples given above are not exhaustive.** **The definition of “sensitive data” needs to be used to determine if data in the software product qualifies as “sensitive data”.**		

Sensitive Resource Categories

The following table depicts general categories of sensitive resources that could be present in the software. This list is intended to be used as a guide, and it is non-exhaustive. **The defining factor of a sensitive resource is its definition.**

Software vendors need to conduct a thorough review of the resources stored, processed, and/or transmitted by the software to identify all forms of sensitive resources that require protection, and implement security controls (including those defined within the standard) as appropriate to protect such information. Software vendors and software assessors work together to validate the sensitive resources of the software and the protection mechanisms employed.

Table 3: Sensitive Resource Categories

Sensitive Resource Categories	Description	Minimum Required Protection Type
Access Control Lists (ACLs)	Resource with permission attributions.	C & I
Certificates	Generally used in the form of public key certificates to bind a public key to an identity.	I

Sensitive Resource Categories	Description	Minimum Required Protection Type
Configuration Settings / Files	Anything in this regard related to sensitive assets.	C & I
Lists	Expressly permitted or prohibited lists. Commonly referred to as whitelists/blacklists. These could be associated with ACL controls, input validation, etc.	I
Records of access to sensitive modes of operation	Recorded activity of both failed attempts and successful access to sensitive modes of operation of the software.	C & I+
Records of suspected anomalous behavior events	Recorded activity of suspected anomalous behavior/events.	C & I+
This table is not exhaustive. The definition of "sensitive resource" needs to be used to determine if resources of the software product qualify as a "sensitive resource".		

Sensitive Functionality Categories

The following tables depict general categories of sensitive functionality and sensitive modes of operation that may be present in the software. Sensitive functionality is generally implemented, for example, as a procedure, method, subroutine, API, function, service, process, or equivalent behavior in the software. This list is intended to be used as a guide, and it is non-exhaustive. **The defining factor of sensitive functionality and sensitive modes of operation is their definitions.**

Software vendors need to conduct a thorough review of the software to identify all forms of sensitive functionality, including sensitive modes of operation. Software vendors and software assessors work together to validate the sensitive functionality of the software.

Table 4: Sensitive Functionality Categories

Sensitive Functionality Context	Description
Account Data Operations	Functionality related to the storage, processing, and/or transmission of account data, including CHD, PAN, and/or SAD.
Authentication and/or Authorization Operations	Functionality related to accessing and/or using sensitive assets. E.g., access to a sensitive mode of operation, access to sensitive {data, resources, and/or functionality}, establishing secure channels, verifying an entity or service, etc. ***Note**: This does not refer to the context of authorization related to a payment transaction.*
Cryptographic Operations	Functionality related to cryptographic operations associated with sensitive assets. E.g., encryption, decryption, signature verification, key generation, etc.

Sensitive Functionality Context	Description
Integrity Validation	Functionality related to integrity validation as it pertains to sensitive assets. This may partially overlap with cryptographic operations depending on the context. E.g., certificate validation, file integrity, data integrity, software updates, etc.
Key Management Operations	Functionality related to cryptographic key-management operations as it pertains to sensitive assets. This may overlap with cryptographic operations depending on the context. E.g., key generation, key conveyance, key destruction, key storage, key check values, etc.
Random Number Functions	Functionality related to random numbers as it pertains to sensitive assets. This may partially overlap with cryptographic operations and/or key management depending on the context. E.g., creating seed values, seeding an RNG, RNG output, key generation, etc.
Secure Channels	Functionality related to secure channels as it pertains to sensitive assets. E.g., establishing a secure channel, transmission over a secure channel, management of a secure channel, removing a secure channel, etc.
Software Protection/Defense Mechanisms	Functionality related to mechanisms implemented in the software to protect and/or defend itself, including its underlying sensitive assets. E.g., input validation, protecting/detecting/recording related to anomalous behavior, error/exception handling, code obfuscation, tamper detection, anti-reverse engineering, compartmentalization, etc.
This table is not exhaustive. The examples given above are not exhaustive. **The definition of ‘sensitive functionality’ needs to be used to determine if functionality of the software product qualifies as ‘sensitive functionality’.**	

Table 5: Sensitive Modes of Operation Categories

Sensitive Modes of Operation Context	Description
Privileged Modes / State	Functionality involving privileged modes, or a state of the software product related to sensitive assets. E.g., administrative, debugging, logs/records, key establishment/loading, remote access, software configuration/updates, etc.
This table is not exhaustive. The examples given above are not exhaustive. **The definition of “sensitive mode of operation” needs to be used to determine if functionality in the software product qualifies as a “sensitive mode of operation”.**	

Account Data

The protection and handling of Account Data, if present in the software, is intended to align with the minimum baseline expectations as detailed in the latest version of the *PCI Data Security Standard* (PCI DSS).

Table 6: Account Data

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data (SAD) includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

The primary account number (PAN) is the defining factor for cardholder data. The term account data, therefore, covers the following: the full PAN, any other elements of cardholder data that are present with the PAN, and any elements of sensitive authentication data (SAD).

If the cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the software, they must be protected in accordance with the requirements for cardholder data.

As in *PCI DSS*, this standard includes requirements that specifically refer to account data, cardholder data, and sensitive authentication data. It is important to note that each of these types of data are different, and the terms are not interchangeable. Specific references to account data, cardholder data, or sensitive authentication data are purposeful, and the context applies specifically to the type of data that is referenced.

Table 7 identifies the elements of cardholder data and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be rendered unreadable—for example, with strong cryptography—when stored. This table is not exhaustive and is presented to illustrate only how storage applies to the different data elements.

Table 7. Account Data Element Storage Requirements

		Data Elements	Storage Restrictions	Required to Render Stored Data Unreadable	DSS Requirements
Account Data	Cardholder Data	Primary Account Number (PAN)	Storage is kept to a minimum	Yes[1,2]	Requirement 3: Protect Stored Account Data[3]
		Cardholder Name	Storage is kept to a minimum[4]	No	
		Service Code			
		Expiration Date			

[1] Refer to the latest version of PCI DSS for acceptable methods to render stored PAN unreadable.

[2] If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable.

[3] Refer to the latest version of PCI DSS and the requirements applicable to account data.

[4] Where the data exists with PAN.

		Data Elements	Storage Restrictions	Required to Render Stored Data Unreadable	DSS Requirements
	Sensitive Authentication Data	Full Track Data	Cannot be stored after authorization[5,6]	Yes, data stored until authorization is complete must be protected with strong cryptography	
		Card verification code			
		PIN/PIN Block			

EMV® 3-D Secure

For software involved with EMV® 3-D Secure (3DS), refer to the *PCI 3DS Data Matrix* in the PCI SSC Document Library to assist in identifying 3DS-related sensitive data that may be present and in scope of the software assessment.

[5] Sensitive authentication data must not be stored after authorization, even if encrypted. This applies even where there is no PAN present.

[6] Except as permitted for issuers and companies that support issuing services.

Appendix A: Sensitive Assets – Assessment Information

This appendix is an optional tool for the software vendor should they choose to use it.
This appendix is not required to be completed by assessors.

The following tables are provided as a tool to provide a templated format, should the software vendor choose to use them to help provide information to their software assessor to facilitate the assessment process. While the software vendor is not required to complete these tables in the format shown, the information being requested in the tables will ultimately need to be provided as part of the software assessment.

The software vendor can extract the following pages and tables and/or otherwise provide this information within their own documentation to their assessor for their software assessment. The vendor can choose the format or manner that they provide this information to their assessor.

Do NOT use any PCI or PCI SSC-affiliated logos, headers, footers, or otherwise on any of the following pages.

Optional Software Vendor Title Page

Software Vendor Name:

Software Name:

Date:

Table A1: Software Vendor Document Information

<table>
<tr><th colspan="4">Software Vendor Document Information</th></tr>
<tr><td colspan="4">This table is provided to facilitate the required documentation for the software assessment, as well as make it easier to reference the documentation in association with the required information, in part as is present in the additional tables in this Appendix.
<b>Document ID:</b> Self-assigned unique identifier used to allow for references to entries in this table.
<b>Document Name:</b> Name of the document.
<b>Date / Version:</b> The date and/or version number of the document.
<b>Description</b>: Describe the general content of the document and how it pertains to the software assessment.</td></tr>
<tr><th>Document ID</th><th>Document Name</th><th>Date / Version</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

Table A2: Cryptographic Key Information

<table>
<tr><th colspan="8">Cryptographic Key Information</th></tr>
<tr><td colspan="8"><b>PCI Secure Software Requirements – This table is used to capture required information pertaining to requirements: 2-1.8[.x]</b>
<b>List all cryptographic key types used by the software that are associated with sensitive assets.</b></td></tr>
<tr><td colspan="5"><b>Key ID:</b> Self-assigned unique identifier used for references to entries in this table.
<b>Key Type:</b> E.g., DEK, KEK, PEK, MAC, Public, Private, etc.
<b>Algorithm:</b> E.g., AES, RSA, DSA, etc.
<b>Key Mgmt:</b> E.g., DUKPT, MK/SK, Fixed, One-time use, etc.</td><td colspan="3"><b>Key Length:</b> Full length (<i>include parity bits as applicable</i>)
<b>Key Generation:</b> Generation method/origin
<b>Key Destruction:</b> List destruction methods <b><i>for each</i></b> storage method
<b><i>Note:</i></b> <i>As cryptographic keys are sensitive data, additional attributes for keys are accounted for in Table A3, which includes their storage location.</i></td></tr>
<tr><th>Key ID</th><th>Key Type</th><th>Algorithm</th><th>Key Mgmt</th><th>Key Length (bits)</th><th colspan="3">Fill out all the information below for each key type</th></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td><td colspan="2"><b>Description & Purpose:</b></td><td></td></tr>
<tr><td rowspan="2"><b>KEY</b></td><td><b>Generation:</b></td><td></td></tr>
<tr><td><b>Destruction:</b></td><td></td></tr>
</table>

Table A3: Sensitive Data Information

Sensitive Data Information

PCI Secure Software Requirements – This table is used to capture required information pertaining to requirements: 2-1, 2-1.1, 2-1.2

Sensitive Data ID: Self-assigned unique identifier used to allow for references to entries in this table.

Sensitive Data Type: The type of sensitive data. Refer to the “Sensitive Data Categories” section in this document as a guide.

Sensitive Data Element: Specific sensitive data element in relation to the Sensitive Data Type.

Stored: Indicate with a ‘Yes’ or ‘No’ if the data element is stored.

Storage Locations: If stored, then denote the location(s) where the data is stored persistently. Else if not stored, denote ‘N/A’.

Key ID: If the data element is a cryptographic key, populate the Key ID from Table A2. Else, denote ‘N/A’.

Doc ID: As applicable, references to entries in Table A1.

Description / Use: Concisely describe the purpose/use of the sensitive data element within/by the software.

Sensitive Data ID	Sensitive Data Type	Sensitive Data Element	Stored	Storage Location(s)	Key ID	Doc ID	Description / Use

Table A4: Sensitive Resource Information

Sensitive Resource Information

PCI Secure Software Requirements – This table is used to capture required information pertaining to requirements: 2-2, 2-2.1, 2-2.2., 2-2.3

Sensitive Resource ID: Self-assigned identifier that can be used to allow for references to entries in this table.

Sensitive Resource Type: The type of resource. Refer to the “Sensitive Resource Categories” section in this document as a guide.

Sensitive Resource Name: Unique identifier (names) of the individual resource in relation to the Sensitive Resource Type.

Stored: Indicate with a ‘Yes’ or ‘No’ if the sensitive resource is stored.

Storage Locations: If stored, then denote the location(s) where the sensitive resource is stored persistently. Else if not stored, denote ‘N/A’.

Sensitive Data: If there are sensitive data elements associated with the sensitive resource, denote the Sensitive Data IDs. Else denote ‘N/A’.

Doc ID: As applicable, references to entries in Table A1.

Description / Use: Concisely describe the purpose/use of the sensitive resource within/by the software.

Sensitive Resource ID	Sensitive Resource Name	Sensitive Resource Type	Stored	Storage Location(s)	Sensitive Data IDs	Doc ID	Describe the purpose/use of the sensitive resource

Table A5: Sensitive Functionality Information

Sensitive Functionality Information

PCI Secure Software Requirements – This table is used to capture required information pertaining to requirements: 2-3, 2-3.1, 2-3.2, 2-3.4, 2-3.5, 2-3.6

Sensitive Funct. ID: Self-assigned unique identifier used to allow for references to entries in this table.
Sensitive Funct. Cat.: The categorial type of functionality. Refer to the “Sensitive Functionality Categories” section in this document as a guide.
Sensitive Funct. Name: Unique identifier (names) of the functionality in relation to the Sensitive Functionality Type, e.g., name of the function, process, etc.
Sensitive Data IDs: If sensitive data is associated with the functionality, enter the Sensitive Data IDs from Table A3. Else denote ‘N/A’.
Sensitive Resource IDs: If sensitive resources are associated with the functionality, enter the Sensitive Resource IDs from Table A4. Else denote ‘N/A’.
Externally Accessible: Indicate with a ‘Yes’ or ‘No’ if the functionality is externally accessible, e.g., as an API.
Sens. Mode of Op.: Indicate with a ‘Yes’ or ‘No’ if the functionality is a sensitive mode of operation.
Doc ID: As applicable, references to entries in Table A1.
Description / Use: Describe the purpose/use of the sensitive functionality within/by the software.

Sensitive Funct. ID	Sensitive Funct. Name	Sensitive Funct. Cat.	Sensitive Data IDs	Sensitive Resource IDs	Externally Accessible	Sens. Mode of Op.	Doc ID	Describe the purpose/use of the sensitive functionality

Table A6: Sensitive Data and Resource Protection Information

Sensitive Data and Resource Protection Information

PCI Secure Software Requirements – This table is used to capture required information pertaining to requirements: 2-1.5, 2-1.6, 2-2.6, 2-2.7

Sensitive Data ID: Reference to entries in the Sensitive Data Information table. Enter as many IDs as pertains to the same parameters for that row.
Sensitive Res. ID: Reference to entries in the Sensitive Resource Information table. Enter as many IDs as pertains to the same parameters for that row.
Protection Categories: Indicates the associated protection attributes, e.g., confidentiality and/or integrity protection. See Table 1.
Protection Methods: Indicates the general method of protection, e.g., encrypted, truncated, hashed, etc.
Key ID: If the data is protected by a cryptographic key, populate the Key ID from Table A2.
Sen. **Funct. ID:** If the security mechanism pertains to Sensitive Functionality in Table A5, document the Sensitive Functionality ID.
Doc ID#: As applicable, references to entries in Table A1.
Description: Concisely describe the security mechanism used to protect the sensitive data/resource.

Sensitive Data ID	Sensitive Res. ID	Protection Categories	Protection Methods	Key ID(s)	Sens. Funct. ID	Doc ID	Description of security mechanism(s) implemented to protect the Sensitive Data / Resource

Table A7: Sensitive Data & Resource Retention & Deletion Information

Sensitive Data / Resource Retention & Deletion Information

PCI Secure Software Requirements – This table is used to capture required information pertaining to requirements: 2-1.3[.x], 2-2.4[.x]

Sensitive Data ID: Reference to entries in the Sensitive Data Information table. Enter as many IDs as pertains to the same parameters for that row.

Sensitive Resource ID: Reference to entries in the Sensitive Resource Information table. Enter as many IDs as pertains to the same parameters for that row.

Configurable Retention: Indicate 'Yes' or 'No' if the retention period is configurable after the software is deployed (in use).

Retention Period: Denote the retention period. If configurable, denote if there is a defined range of allowable periods/settings.

Sen. Funct. ID: If the retention and/or deletion mechanism pertains to Sensitive Functionality in Table A7, document the Sensitive Functionality ID.

Doc ID: As applicable, references to entries in Table A1.

Deletion Method: Describe the method used to securely delete the sensitive asset or otherwise render it unrecoverable when it is no longer required.

Sensitive Data ID	Sensitive Resource ID	Configurable Retention	Retention Period(s)	Sens. Funct. ID	Doc ID	Describe the Retention and Deletion Methods

Table A8: Sensitive Asset Flows

Sensitive Asset Flows

PCI Secure Software Requirements – This is required information pertaining to requirements: 2-1.7, 2-2.8

Provide flow diagrams that show the details of all sensitive asset flows. The ID#s from the previous tables should be used for easier references in the diagram(s).

For each sensitive asset flow, identify the following:

- The sensitive data involved.
- The sensitive resources involved.
- The sensitive functionality involved, including all sensitive modes of operation.
- All components involved in the storage, processing, and/or transmission of the sensitive assets above.

Specify all types of sensitive asset flows, including any output to hardcopy, paper, or other external media. Sensitive asset flows must also denote locations where sensitive assets cross trust boundaries and where it is passed to other applications or services that were not included in the assessment.

Note: There are no row entries for this table. The instructions above are intended to facilitate the required flow diagrams.