**PCI-DSS SAQ B-IP (End-to-End Encryption)
Review & Attestation Worksheet**

**Agency/Department Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Scope Description –** May be defined as offices, divisions or merchant numbers. Please attach additional page if necessary: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

In an effort to ensure proper due diligence in the completion of PCI Self-Assessment Questionnaires (SAQ), Agency and DTS Personnel will review the SAQ requirements applicable to that person’s job function. The DTS IT Director should manage the DTS Review and then provide this document to the agency for an Agency Review and completion of the SAQ.

* The appropriate employee will only sign off on requirements after proper review and testing of associated components as directed by the SAQ.
* Do not complete the SAQ until after reviews as outlined in the worksheet have been completed.
* Personnel will also verify necessary documentation is in place and known to affected parties on the requirements pertaining to specific job functions.
* If more than one person for a job function needs to complete a review, please use the Signature Overflow Page to collect additional signatures.
* This document will be submitted with the SAQ to the Agency Finance Director for review.
* The Agency Finance Director will then submit this document along with the SAQ and other required documentation to the State Finance PCI Compliance Coordinator.

**DTS REVIEW**

**IT Director** Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. To your knowledge, has the agency provided an accurate list of end-point components in the PCI scope? YES/NO
2. Have the identified devices been mapped to ensure all connected network and server devices are considered in the PCI scope? YES/NO
3. Does the agency’s SLA with DTS cover all activities requiring PCI-DSS compliance? YES/NO

IT Director Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**AGENCY REVIEW**

**Division/Department Functional Manager** Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The Division/Department Functional manager is the agency employee charged with policy creation and managing PCI in the division or department.

1. To your knowledge has the agency provided an accurate list of end-point components in the PCI scope to DTS? YES/NO
2. Does the agency’s SLA with DTS cover all activities requiring PCI-DSS compliance? YES/NO
3. Does the agency have an active policy that is known to all affected parties and addresses all applicable elements of PCI-DSS requirements? YES/NO
4. I have reviewed the following list of requirements, have ensured the necessary testing has been performed and have reviewed documented policies and procedures to ensure the SAQ results are accurate.

Requirements: 3.2, 9.9.1, 9.9.3, 12.X

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Functional Manager** Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The Functional Manager is the agency employee charged with managing operations within the department or office where credit cards are accepted. The Functional Manager may also oversee field offices where credit cards are accepted.

1. I have reviewed the following list of requirements, have ensured the necessary testing has been performed and have reviewed documented policies and procedures to ensure the SAQ results are accurate.
2. Where applicable, I have confirmed that field offices are operating in compliance with agency policies and the requirements listed below.

Requirements: 3.2 - 3.3, 9.5 - 9.9, 9.9.2

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NOTE: If needed, agency management may require field office managers to individually sign off on requirements in the Functional manager section. Please use the Signature Overflow Page in this instance.

**Signature Overflow Page**

|  |  |  |  |
| --- | --- | --- | --- |
| PRINT NAME | JOB FUNCTION | SIGNATURE | REQUIREMENTS TESTED |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**SAQ B-IP for E2EE Compliance Notes**

* Requirements 3.x, 9.5-9.8.1: These requirements are only applicable IF card data is written down. The card terminals do not store any data.
* Requirement 4.1: The answer is marked yes, because it is part of the E2EE solution.
* Requirement 4.2: Please place in your policy and train personnel not to send card information through any messaging service.
* Requirement 9.9.x: Please make sure the agency has a policy and practice of periodically inspecting devices for tampering. Defining "Periodically" is a business decision that should be based on security controls surrounding the devices and volume of use.
* Requirement 12.x: Applicable requirements should be addressed in the agency’s security policy.
* Requirement 12.8.x: These requirements are marked yes, because the E2EE solution the State uses is managed as part of the current merchant services contract with Chase Paymentech.