**PCI-DSS SAQ D for Chase Mobile
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.

**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 (NOTE: This includes ensuring DTS has adequate policies in place to meet requirements that are not controlled by the agency)? YES/NO
4. Are all the mobile devices used for the acceptance of credit cards State-owned and registered in MDM? YES/NO
5. 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.

Agency Requirements: 2.X, 3.7, 5.X, 6.1-6.2, 6.7, 7.1, 7.3, 8.2, 8.3, 8.4, 8.5, 8.8, 9.2, 9.9.1, 9.9.3-9.10, 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.X, 8.1.1, 9.1.3, 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 D for Chase Mobile Compliance Notes**

* Requirements 2.2, 5.x: If the agency is not keying transactions, meaning EVERY transaction is swiped, these requirements are not applicable. If the agency is keying (manually entering) card data, the agency must assign a person who is “knowledgeable about common security parameter settings” to harden the devices per the [Division of Finance Mobile Standards Document](http://finance.utah.gov/reporting/documents/Chase%20Mobile%20Standards%20Document%20v1.0.docx) in order to be compliant.
* Requirement 2.4: The agency must retain an inventory of devices. This inventory should include both mobile and swipe devices used for accepting cards. The inventory should include make, model and serial number.
* Requirements 3.x, 9.2, 9.5-9.8.1: These requirements are only applicable IF card data is written down. The Chase Mobile application does not store any data.
* Requirement 4.2: Please place in your policy and train personnel not to send card information through any messaging service.
* Requirement 6.2: Please ensure policy and practice involve keeping apps and OS updates current on mobile devices accepting credit cards.
* Requirements 6.1, 7.1.4: These requirements are marked yes, because the Division of Finance provides these controls.
* Requirements 2.1(b) 8.x: Applicable to the Chase Mobile application. You can have a single device password/PIN as long as you have separate and unique authentication for each user on Chase Mobile. The single device authentication should be changed, though, if users with device access are terminated or reassigned. Answers that are already marked yes are managed by Chase Mobile application requirements.
* Requirement 9.1.3: Must restrict physical access to the mobile devices used for accepting credit cards.
* Requirement 9.8.2: Mobile devices must be wiped via MDM and restored to default when they will no longer be used for card acceptance.
* 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.