



STATE OF MISSISSIPPI
HALEY BARBOUR, GOVERNOR

DEPARTMENT OF FINANCE AND ADMINISTRATION

KEVIN J. UPCHURCH
EXECUTIVE DIRECTOR

To: Agency Executive Directors
Agency Accounting Directors
Agency IT Directors

From: Cille Litchfield, Deputy Executive Director

Date: June 22, 2009

Re: Payment Card Industry (PCI) Compliance Audit Services

The Payment Card Industry (PCI) Data Security Standard (DSS) compliance is a mandatory requirement for all transactions involving major credit card vendors, online merchants and service providers. Its purpose is to create common industry security requirements to protect cardholder data. The standard was developed by the founding payment brands of the PCI Security Standards Council, including MasterCard, Visa, American Express, Discover and others, to help facilitate the broad adoption of consistent data security measures on a global basis. The core of PCI-DSS is a group of principles and accompanying requirements.

The standard applies to all merchants and service providers that process, transmit, or store cardholder information. It applies to all payment channels including mail, telephone, and e-commerce. PCI-DSS also requires merchants and service providers to perform security scans every 90 days on all internet facing networks and systems. The goal of this review of security practices is to ensure that we are all doing everything we can to minimize process vulnerabilities and reduce the chance of breaches, fraud, and financial loss related to cardholder data.

To validate compliance, all merchants and service providers, regardless of credit card transaction volume and payment channel, must fulfill a series of validation actions. Once the validation actions have been performed and are found to be compliant, both merchants and service providers must provide the appropriate **Attestation of Compliance** document to their acquirer and the Department of Finance and Administration (DFA). Failure to comply with these requirements can result in steep fines, restrictions, or even expulsion from card acceptance programs.

By complying with these requirements, merchants and service providers not only meet their obligations to PCI-DSS, but also build a culture of security that benefits all parties.

There are four levels of PCI compliance for merchants. Currently the majority of State of Mississippi agencies accepting credit cards as a form of payment operate internet facing transactions (card not present) as a Level 3 Merchant (20,000-150,000 transactions per year) using a single payment processor. This level of PCI compliance requires:

- Annual Self-Assessment Questionnaires (SAQ) validated by the Merchant, and
- Quarterly network scans validated by a Qualified Independent Scan Vendor.

Additionally, a number of Mississippi agencies have individual agreements with other card processors/service providers and:

- ❑ Offer web facing applications (Tax Commission),
- ❑ Offer customer facing Point-of-Sale transactions (Department of Wildlife, Fisheries and Parks, Secretary of State, Department of Transportation, Department of Health), or
- ❑ Offer a combination of internet facing and other card processor/service providers (Department of Health, and Department of Wildlife, Fisheries and Parks).

Regardless of the above merchant level your agency falls within:

- ❑ Agencies are responsible for quarterly PCI-DSS scans
- ❑ Agencies are responsible for completion of the annual SAQ and must provide the appropriate Attestation of Compliance to PCI-DSS to their acquirer and DFA
- ❑ If an agency's application is hosted at ITS, ITS is responsible for quarterly scans
- ❑ If the agency's application is hosted by the agency, the agency is responsible for quarterly PCI-DSS scans
- ❑ If the agency's application is hosted by a 3rd party vendor, the agency is responsible for quarterly PCI-DSS scans.
- ❑ All agencies, regardless of where their application resides (is hosted), must use the available Coalfire System, Inc. services procured by ITS on behalf of state entities for scans and SAQ completion.

If your agency accepts credit cards as a form of payment as one or more of the merchant levels above, you are required to participate and comply with the PCI-DSS standards for your agency's level of credit card acceptance. The Mississippi Department of Information Technology Services (ITS), in conjunction with the DFA, has established a procurement vehicle for use in obtaining PCI compliance audit services. The available services were procured by ITS on behalf of state entities via Request for Proposal No. 3532 and meet Mississippi's requirements for legal purchases.

To assist agencies in complying with PCI–DSS mandates, state agencies will use Project Number 37081, a Professional Services Agreement Between Coalfire Systems, Inc. and the Mississippi Department of Information Technology Services on Behalf of the Agencies and Institutions of the State of Mississippi. To request services under this agreement go to <http://www.its.ms.gov/PCI.shtml>.

Agencies should also reference DFA's proposed administrative rule [Payments by Credit Card, Charge Card, Debit Cards or other Forms of Electronic Payment of Amounts Owed to State Agencies](#) found on the MMRS website at www.mmrs.state.ms.us.

Agencies should complete [#2551MMRS PCI Security Contact Maintenance Form](#), located on the MMRS website on the E-Payment Services page at www.mmrs.state.ms.us to authorize specific staff to access the PCI SAQ portal and view IP address scan results and remediation recommendations.

Questions should be directed to the MMRS Call Center at 601-359-1343 or via email at mash@dfa.state.ms.us.