MISSISSIPPI DEPARTMENT OF FINANCE AND ADMINISTRATION
ADMINISTRATIVE RULE
PAYMENTS BY CREDIT CARD, CHARGE CARD, DEBIT CARDS OR OTHER FORMS OF ELECTRONIC PAYMENT OF AMOUNTS OWED TO STATE AGENCIES

The Department of Finance and Administration (DFA) has established the following Administrative rule to be followed when agencies, in accordance with §27-104-33, Mississippi Code of 1972, Annotated, elect to accept payments by credit cards, charge cards, debit cards, electronic check and other forms of electronic payment for various services and fees collectible for agency purposes.

I. Definitions

A. Electronic payments: Consumer and business initiated payments, whether made through the Internet or in person, for various services and fees using any of the following payment instruments: credit cards, bank cards, charge cards, debit cards, electronic checks, direct debits via electronic funds transfer.

B. ACH: Automated Clearing House. Affiliated with the U. S. Treasury and the Federal Reserve System and used as the conduit for electronic payments and collections. The ACH is the settlement vehicle for electronic payments. The ACH is also used to transport direct debit and credit transactions to consumer bank accounts.

C. Application Service Provider (ASP): An application service provider (ASP) provides computer-based services to customers over a network. The most limited definition is that of providing access to a particular application program (such as license renewals, registrations, etc.) using a standard protocol such as HTTP. ASP applications for purposes of this rule are those which accept electronic payments either through a browser-based application, or other revenue input sources.

D. DFA: Mississippi Department of Finance and Administration.

E. EOC FEE: Electronic Government Oversight Committee (EOC) Fee. This fee is used to offset the costs associated with providing electronic services and operating the electronic portal (www.mississippi.gov) at ITS. §25-53-151 (2) of the Mississippi Code defines the EOC. All transactions must include an EOC fee unless ITS has granted express written exemption of this fee for a specific Agency application or has granted approval for the Agency to absorb and directly remit the EOC fees associated with transactions for a specific application to DFA payable to State Treasury Fund 3126.

F. Consumer: Consumer, for purposes of these rules, may be any individual person or business representative who initiates a transaction involving electronic payment.

G. Convenience Fee: Convenience fee is the payment-processing fee as calculated and approved by the Department of Finance and Administration (DFA). No other fees, including the EOC fee, will be defined as convenience fees. All transactions must include a convenience fee unless DFA has granted express written approval for the Agency to absorb the payment processing costs associated with the transactions for a specific transaction and for the agency to remit those fees to DFA payable to State Treasury Fund 3126.

H. ITS: Mississippi Department of Information Technology Services.

I. Point of Sale: Point of Sale (POS). Payments made "over the counter" for fees for services. For the purposes of electronic payments in Mississippi, agencies desiring to accept "over the counter" electronic payments must have a POS application. POS applications may be: A web-based system where all payment information is keyed into the application by the client or a "card swipe" application similar to those found in commercial enterprises. POS applications must be certified to meet PCI Compliance Standards.

J. SAAS: Statewide Automated Accounting System.

K. SPI: SAAS Payment Interface. The SPI defines the accounting entries used to record all electronic payment transactions.

L. Record Keeping: An agency must establish and maintain financial records and keep them available for the purposes of audit. The record keeping procedures must include the capture of the details of the electronic payments, associated fees, and supporting reconciliation documentation.

M. Payment Card Industry – Data Security Standards: PCI-DSS is the result of collaboration between the major credit card brands to develop a single approach to safeguarding sensitive data. PCI-DSS defines a series of requirements for handling, transmitting, and storing sensitive data.

The PCI-DSS standards can be found at https://www.**pci**securitystandards.org/ .

N. Self-Assessment Questionnaire (SAQ): The PCI Data Security Standard Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

O. Payment Application Approved Scanning Vendor (PA-ASV): Organizations that validate adherence to certain DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers.

P. Payment Application Qualified Security Assessor (PA-QSA): Companies or employees that have been certified by the Payment Card Industry Security Standards Council to validate an entity's adherence to the PCI PA-DSS.

Q. Cardholder Data: Data that includes cardholder full name, full account number, expiration date, service code, full magnetic stripe, PIN/PIM Block or Card Validation Code (e.g., three-digit or four-digit value printed on the front or back of a payment card). Card Validation Code is also known as the CVV2 or CVC2 code.

R. Sensitive Cardholder Data: Data includes Card Validation Code (e.g., three-digit or four digit value printed on the front or back of the payment card (e.g., CVV2 and CVC2 data)).

S. Payment Application Data Security Standards (PA-DSS): A program managed by the Payment Card Industry Security Standards Council (PCI SSC). PA DSS is a set of standards designed to assist software vendors in developing secure payment applications that comply with PCI-DSS requirements.

The PA-DSS standards can be found at https://www.pcisecuritystandards.org/ .

T. Revenue Input Source: Electronic transactions from Web-based, Point of Sale (POS), Interactive Voice Response (IVR), Over the Counter Sales, etc.

U. 27-104-33. Payment by Credit card, charge card, debit card, or other form of electronic payment amounts owed to state agencies.

The State Department of Finance and Administration shall establish policies that allow the payment of various fees and other accounts receivable to state agencies by credit cards, charge cards, debit cards and other forms of electronic payment in the discretion of the department. Any fees or charges associated with the use of such electronic payments shall be assessed to the user of the electronic payment as an additional charge for processing the electronic payment.

Agencies with the approval of the Department of Finance and Administration may bear the full cost of processing such electronic payment if the agency can demonstrate to the department's satisfaction that they are able to assume these costs and provide the related service for the same or lesser cost.

II. Payment Applications - Fees Paid By Consumer

A. Agency applications accepting payments shall use the third party electronic payment processor designated by DFA to accept electronic payments for various services and fees collectible for agency purposes unless express written approval is given by DFA for the use of an alternate payment processor.

1. Designated payment processor is to be used regardless of where the application is hosted (agency, ITS, third-party).

2. Rules for obtaining approval of an alternate payment processor are found in Section IV.

B. The services provided by the processor and the fees for such services shall be set forth in the contract approved by the State. All such agreements are considered e-government agreements and are under the purview of ITS (see 001-020 Acquisitions within ITS Purview, item 3, in the ITS Procurement Handbook).

C. Funds will be deposited in the account designated by the State Treasurer and transferred to the designated agency funds in SAAS once the bank deposit is balanced.

D. The payment processor will support, as a separate line item on the transaction payment summary presented to the customer, the convenience fee for the service and fee payment due the agency.

E. DFA will provide the software components to be used by agency applications in calculation of the convenience fee associated with a particular fee or services payment.

1. The standard calculation used by the software ensures the total cost to process the electronic payment is passed to the consumer.

2. The software components are collectively known as the "charges client".

F. The application must inform the consumer of the total amount of the convenience fee that will be added to the fee or service billing before such charges are assessed. The consumer must be able to cancel the transaction at this point without any fee being assessed.

G. The convenience fee and EOC fee shall be plainly included and identified on the electronic receipt provided to the consumer.

H. The convenience fee charged to the consumer and noted in the financial records for verification purposes:

1. Will be recorded in SAAS as a revenue receipt in DFA fund 3126 (known as the Mississippi.Gov Portal fees Fund).

2. Will not flow through agency accounting journals.

I. The portion of the convenience fee owed the electronic payment processor shall be directly withheld by the processor, then aggregated with other fees for that application and recorded appropriately as an expenditure transaction against the Mississippi.Gov Portal Fees Fund.

J. Any rejected items returned to DFA by the designated third party processor will be forwarded to the appropriate agency for handling after being netted out of the settlement for the day.

K. Revenues for all fees and services shall be recorded at gross in SAAS as revenue, as specified by the agency on the SAAS electronic payment distribution tables.

L. Actual processing costs to include fees for authorization, settlement, and Electronic Government Oversight fees, will be recorded as expenditures as specified by the Agency on the SAAS electronic payment distribution tables.

III. Payment Applications - Fees Paid By Agency

A. Agencies desiring to pay all fees associated with electronic processing of payments must demonstrate to DFA their ability to do so and receive express written approval from DFA. Requirements for requesting approval are outlined in section VI of these rules.

B. Agency applications accepting payments shall use the third party electronic payment processor designated by DFA to accept electronic payments for various services and fees collectible for agency purposes unless express written approval is given by DFA for the use of an alternate payment processor.

1. Designated payment processor is to be used regardless of whether the particular application is a POS application, an application hosted through the Mississippi.gov infrastructure, or an application hosted through other ASPs.

2. Rules for obtaining approval of an alternate payment processor are found in section IV.

C. The services provided by the processor and the fees for such services shall be set forth in the contract approved by the State. All such agreements are considered e-government agreements and are under the purview of ITS (see 001-020 Acquisitions within ITS Purview, item 3, in the ITS Procurement Handbook).
http://dsitspe01.its.ms.gov/its/procman.nsf/TOC4?OpenView

D. Funds will be deposited in the account designated by the State Treasurer and transferred to the designated agency funds in SAAS once the bank deposit is balanced.

E. Revenues for all fees and services shall be recorded at gross in SAAS as revenue as specified by the agency on the SAAS electronic payment distribution tables.

F. Actual processing fees to include fees for authorization, settlement, and Electronic Government Oversight fees, will be recorded as expenditures as specified by the agency on the SPI distribution tables. These fees will be applied against the day's settlement for the agency.

G. Any rejected items returned by the designated third party credit card/or other electronic processor to DFA will be forwarded to the appropriate agency for handling after being netted out of the settlement for the day.

IV. Approval of an Alternate Payment Processor

A. An agency wishing to use an alternate payment processor must submit a written request to the Department of Finance and Administration, Director, Office of Fiscal Management, 501 North West Street, Suite 701 - D, Jackson, MS 39201.

B. The written request must state:

1. The reason(s) the State-approved payment processor is not suitable for the agency application.

2. The impact if the request is not granted.

C. The application must be approved by DFA prior to entering into the procurement process for the alternate payment processing services.

D. The agency must state what payment processors are available that meet their needs.

E. The agency must describe the agency application including:

1. The agency program supported.

2. The items (services and fees) offered for sale.

3. The individual item costs.

4. The estimated usage of the processor (i.e., the number of transactions that will occur per fiscal year).

5. An estimate of the processing costs "per transaction" for the items to be sold.

6. The costs associated with the use of an alternate payment processor including, but not limited to, purchased and leased equipment, training, and contractual services.

F. The agency must acknowledge that if DFA approves the agency's request to pursue alternate payment processing services:

1. Funds will be deposited in the account designated by the State Treasurer and transferred to the designated agency funds in SAAS once the bank deposit is reconciled and balanced by the agency. DFA will not perform this reconciliation and will not approve the transfer of funds to SAAS until proof of reconciliation is provided.

2. Any request for an exception to the above reconciliation requirement must be clearly documented in the request for the alternate payment processor.

G. The service must be legally procured following the rules for technology procurement. All such services are considered e-government services, and are within the purview of ITS even if those services are offered at no cost to the agency. (See 001-020 Acquisitions within ITS Purview, item 3, in the ITS Procurement Handbook):
http://dsitspe01.its.ms.gov/its/procman.nsf/TOC4?OpenView

1. DFA will be an active participant in the procurement, implementation, and acceptance of the alternate payment processor before the application supported is certified for production operations.

2. DFA, at its discretion, may require that DFA be a party to the contract.

H. The alternate payment processor and/or 3rd party vendor must work with DFA to interface daily settled transactions and any associated fees into SAAS via the Cash Receipts (CR) interface or the SPI.

I. Agencies are required to collect any State required fees, such as EOC fees.

J. Approval under this section shall not relieve an agency of its responsibility concerning other sections of this rule.

V. Approval for All Fees to Be Paid By Agency

A. An agency wishing to obtain approval to bear the full cost of processing electronic payments should address the written request to the Department of Finance and Administration, Director, Office of Fiscal Management, 501 North West Street, Suite 701 - D, Jackson, MS 39201.

B. The request must state whether the application is web-based or of another type (example: submission of a file of EFT debits for mortgage payments).

C. The agency must describe the agency application including:

1. The agency program supported.

2. The items (services) offered for sale or collections.

3. The individual item costs.

4. An estimate of the processing cost "per transaction" for the items (services) to be sold.

D. The agency must state whether the agency or the consumer will pay the EOC fee.

E. The agency request must clearly:

1. Document whether the request is for an application where the consumer can purchase only a single item or service at a time (example: drivers' license renewals) or a shopping cart model where multiple items may be purchased (example: hunting and fishing).

2. Demonstrate a dollar neutral cost or cost saving to the agency when absorbing the processing fees rather than having the consumer pay the fees projected over a fiscal year. All assumptions must be documented.

3. Demonstrate that the funds to defray the total cost of electronic processing will be available projected over a fiscal year. All assumptions must be documented.

F. The agency must acknowledge that it will be required to set aside cash/authority at a specified minimum limit in a specified fund to cover expenses (debits) associated with the agency's transactions for the following:

1. Authorization and settlements fees
2. Refunds
3. Chargebacks
4. Voids
5. Returned items charges

G. Approval under this section implies that the agency accepts and understands that the application will not be certified for production until such time as complete end-to-end testing is approved by DFA.

1. Testing will include financial settlement testing of all payment types.
2. Testing will include refunds and chargebacks.
3. Testing will include full reconciliation using the procedures developed by the Agency for that purpose.

VI. Waiver of the EOC Fee

All requests to waive EOC fees must be addressed to Department of Information Technology Services, Attention: E-government Oversight Committee, 301 North Lamar Street, Suite 508, Jackson, Ms 39202.

VII. Payment Card Industry – Data Security Standards (PCI-DSS)

A. State agencies accepting credit and/or debit cards will comply with Payment Card Industry – Data Security Standards (PCI- DSS) to safeguard cardholder and sensitive cardholder data, regardless of revenue input source).

B. 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 see http://www.its.ms.gov/PCI.shtml.

1. Agencies will attend a Self-Assessment Workshop.

2. Agencies will complete a Self-Assessment Questionnaire (SAQ) and participate in interviews to evaluate their current operations and network. If an agency accepts credit cards via mail, manually or other non Internet means, the Self-Assessment Questionnaire is still required. Additionally, there may be other operational security issues the agency will need to address.

3. All agencies will have quarterly scans on all Internet-facing Internet Protocol (IP) addresses used in the processing and storing of credit card data under the Professional Services Agreement between Coalfire Systems, Inc. and ITS.

4. Agencies will make a good faith effort to correct deficiencies identified in the remediation plan and provide status or remediation tasks as requested by DFA and ITS.

C. Agencies that do not participate in PCI-DSS cannot accept credit cards/debit cards as a form of payment. If an agency is found accepting credit/debit cards as payment and has not completed the steps for PCI compliance, DFA under the authority of 27-104-33, will issue the agency a cease and desist letter to close the system down. To request an appeal see Section X.

VIII. Development/Hosting Options and Ultimate Responsibility for PCI-DSS and Fines and Penalties

A. Agencies are responsible for ensuring their vendors are PCI-DSS compliant. Vendors will use Payment Application Data Security Standards (PA-DSS) to develop applications. The PA-DSS standards can be found at https://www.**pci**securitystandards.org/ .

B. Should an agency wish to move the hosting of their applications to Mississippi Department of Information Technology Services (ITS), the agency will bear the responsibility and cost to bring the application into PCI compliance before it is transferred to ITS. The agency will ensure the transfer takes place no later than 90 days after the last PCI scan. Since code will change within the application, another scan will occur after the transfer to ITS and the agency will be responsible for all PCI non-compliance items.

C. The following table is a general guideline for PCI-DSS responsibility and liability:

System Type or Web Development/Hosting	Responsible Entity
ITS Developed/ITS Hosted	State is responsible for PCI compliance, fines and penalties
Agency Developed/ITS Hosted	State is responsible for PCI compliance, fines and penalties for state network infrastructure. The agency is responsible for PCI compliance, fines and penalties for the agency application and internal agency business practices.
Agency Developed/Agency Hosted	The agency is responsible for PCI compliance, and all fines and penalties
3rd Party Vendor Developed/Agency Hosted	The agency is responsible for PCI compliance, and all fines and penalties
3rd Party Vendor Developed/ITS Hosted	State is responsible for PCI compliance, fines and penalties for state network infrastructure. The agency is responsible for PCI compliance, fines and penalties for the agency application.
3rd Party Vendor Developed/3rd Party Vendor Hosted	The agency is responsible for PCI compliance and all fines and penalties
Non-Web based systems, Point of Sale (POS), Interactive Voice Response (IVR), Over the Counter Sales, Telephone Sales, Mail in, etc.	The agency is responsible for PCI compliance and all fines and penalties

IX. Security Breaches and Notifications

A. In the event of a security breach, credit card or debit card data could be compromised. Agencies will immediately terminate the application/services to preserve evidence and notify:

1. DFA's Chief Systems Information Officer at 601-359-6570.

2. Mississippi Department of Information Technology Services, Security Division at 601-359-2690 and E-Government at (601) 359-2742.

3. Mississippi State Attorney General's Office, Consumer Protection Division at (601) 359-3680 or 1 (800) 281-4418 and the Cyber Crimes Division at (601) 359-3817.

B. The agency shall notify their customers of the breach once law enforcement informs the agency that customer notification will not impede an investigation.

1. Agencies may notify customers using written notices or electronic notices. As a last resort, telephone notices can be given. Documentation that notices were provided, to whom they were provided, and when such notices were provided must be maintained by the Agency..

2. The notice shall be clear and conspicuous and include:

    a. A description of the incident in general terms.

    b. The type of personal information subjected to unauthorized access or acquisition.

    c. The general acts the agency has taken to protect the information from further unauthorized access.

    d. A telephone number that the customer can call for further information.

    e. Advice that directs the customer to remain vigilant by reviewing account statements and monitoring free credit reports or close an account.

X. Appeal Process

A. An agency wishing to appeal a cease and desist letter must submit a written request to the Department of Finance and Administration, Director, Office of Fiscal Management, 501 North West Street, Suite 701 - D, Jackson, Ms 39201.

B. The agency must provide the following information in the written request:

1. The agency program supported.

2. The items (services) offered for sale or collections.

3. The individual item costs.

4. An estimate of the processing cost “per transaction” for the items (services) to be sold.

5. The number of items sold per year and the total cost of those items.

6. A detailed description of how the system works.

7. A detailed list of software operating on the system.

8. A detailed list of equipment, including the name, model number, and purposed of the equipment.

9. A detailed description of accounting entries made to account for revenue and processing and other fees.

C. The agency must state whether the agency or the consumer pays the EOC fee. The agency request must clearly:

1. Document whether the consumer can purchase only a single item or service at a time (example: drivers' license renewals) or a shopping cart model where multiple items may be purchased (example: hunting and fishing).

2. Demonstrate a dollar neutral cost or cost saving to the agency when absorbing the processing fees rather than having the consumer pay the fees projected over a fiscal year if the agency is to pay the processing fees. All assumptions must be documented.

3. Demonstrate that the funds to defray the total cost of electronic processing will be available projected over a fiscal year if the agency is to pay the processing fees. All assumptions must be documented.

D. If the agency is paying processing fees, the agency must acknowledge that they will be required to set aside cash/authority at a specified minimum limit in a specified fund to cover expenses (debits) associated with the agency's transactions for the following:

1. Authorization and settlements fees

2. Refunds

3. Chargebacks

4. Voids

5. Returned items charges

E. The agency will also submit their PCI Self-Assessment Questionnaire, Remediation Plan, and cost estimates to correct deficiencies identified in the Remediation Plan. Once the agency information is reviewed, the agency will be given a written response to the appeal request.