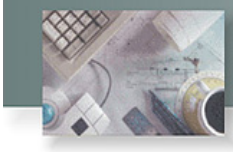

Compliance Component

DEFINITION	
Name	Securing Electronic Transactions
Description	Securing Electronic Transactions provides acceptable methods for agencies or third party vendors handling payment card or electronic transactions for persons conducting business with the state.
Rationale	To protect agencies and citizens using electronic transactions and the integrity of the payment system.
Benefits	• Reduces: o Payment card fraud i.e. unauthorized use of the card o Fraud losses i.e. payment refunds due to unauthorized use o Unanticipated operational expenses o Citizen inconvenience

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Identification and Authentication
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	There are twelve electronic transaction data requirements that must be complied with: 1. Have a current firewall with appropriate configurations 2. Do not use default system passwords 3. Protect stored data 4. Encrypt cardholder data across public networks 5. Have current anti-virus software in place 6. Develop and maintain secure systems and applications 7. Restrict access to data on a need-to-know basis 8. Assign unique user IDs to persons with access 9. Restrict physical access to cardholder data 10. Monitor all access to data 11. Regularly test security systems and processes 12. Maintain a policy that addresses information security The electronic payment information stored by an agency or a vendor on behalf of the agency shall comply with the following requirements:

	• Do not store the following under any circumstances: o Full contents of any track from the magnetic stripe on the back of the card o Card validation code – the three digit value printed on the signature panel • Store only that portion of the customer's account information that is essential to the agency business (i.e. name, account number or expiration date) • Store all material containing this information (i.e. authorization logs, transaction reports or carbons) in a secure area limited to authorized personnel. Destruction of cardholder information • Destroy or purge all media containing obsolete transaction data with cardholder information Use of third party providers • Agencies must maintain documentation of any agent or third party provider that engages in the processing or storage of transaction data on the agencies' behalf. • Agents or third party providers must adhere to all rules and regulations established by the agencies.
Document Source Reference #	VISA version 1.0 December 15,2004

Standard Organization			
Name	Payment Card Industry Data Security Standard	*Website*	http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf
Contact Information			
Government Body			
Name		*Website*	
Contact Information			

KEYWORDS	
List all Keywords	Cardholder, credit card, validation code, accounts, payment, debit card.

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*

Rationale for Component Classification	
Document the Rationale for Component Classification	

Conditional Use Restrictions	
Document the Conditional Use Restrictions	

Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	09/07/06	*Date Accepted / Rejected*	9/12/06
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			