CYBER SECURITY STANDARD

Standard Identifier:	CSS2019-003-PCI
Standard Name:	Payment Card Industry Data Security Standard (PCI-DSS)
Version:	Version 1.0
Cyber Security Framework Alignment:	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders ID.RM-2: Organizational risk tolerance is determined and clearly expressed
Strategic Alignment:	☒ Cyber Risk ☒ Cyber Outreach ☒ Cyber Protection ☐ Cyber Operations
Standard Summary:	PCI-DSS standards are applicable to all agencies within the executive branch of State government that accept or intends to accept card payments. This includes any executive branch entity that stores, processes or transmits cardholder data. (See Definitions.) Agencies must ensure both technical and procedural processes are in place and compliant before accepting customer credit card data.
Standard Details:	• Payment Terminals/readers may not be added to the State network without notifying WVOT and submitting a request through both the Service Desk and Department IRM. Unless otherwise exempt, all equipment must be purchased through the WV State Treasurer's Office (WVSTO) merchant services contract. • Payment Terminals/readers must be routinely examined for evidence of tampering and any evidence brought to the attention of the Agency Compliance Coordinator. • Payment Terminals/readers must be logically separated on the network from non-PCI traffic. • Payment Terminals/readers may only be attached to computers or other devices for the sole purpose of processing credit cards and may not be used as a standard "user machine" or general work PC. • Access to the cardholder data environment must be restricted to only those employees with a need to

	access and physical controls must be in place to protect the cardholder data environment. • A list of Payment Terminals/readers must be maintained and updated yearly. • If any agency needs assistance to identify, correct or assess any PCI-DSS compliance, then the agency must use the PCI consulting services contract established by the WVSTO. • Agencies must complete and submit the appropriate Self-Assessment Questionnaire (SAQ) annually. The agency may use the WVSTO's designated assessment tools contract.
Exceptions Procedure:	WVOT acknowledges that there may be constraints in complying with the standards set forth in meeting this standard. For an agency to receive a temporary exception, agencies must submit a Plan of Action and Milestones that includes the following: • The service, application, vendor, or process causing the constraint. • The estimated timeline to accomplish the compliance • Preventative security measure and mitigation strategy that will be put in place while accepting risk.
Questions or Concerns:	Please contact agency or department Interdepartmental Relationship Managers for questions or concerns. Please reference the Request Number in your inquiry.
Additional PCI-DSS Resources	https://www.pcisecuritystandards.org
Additional WVSTO Contract Resources:	https://www.wvsto.com/Contracts