STATE OF VERMONT
Agency of Human Services (AHS)

Payment Card Industry Data Security Standard Compliance Policy	REVISION HISTORY:	Chapter/Number 5.04
	EFFECTIVE DATE: 10/23/08	Attachments/Related Documents: AHS Incident Response Policy

Authorizing Signature: Cynthia D. LaWare Date Signed: 10/23/08

Cynthia D. LaWare, Secretary, Agency of Human Services

PURPOSE:

The Payment Card Industry (PCI) standard provides an actionable framework for developing a robust account data security process—including preventing, detecting and reacting to security incidents relating to payment card data.

BACKGROUND and REFERENCES:

The State is required to maintain compliance with PCI data security standards when credit card processing may be used in financial transactions. This policy provides explicit guidance for these situations and was created to address the requirements stated by the attestation of compliance required by the Vermont State Treasurer's office.

The Payment Card Industry Data Security Standard
https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

SCOPE:

This document applies to all Agency Departments, Divisions and Offices hereafter referred to jointly as "department".

STANDARDS:

AHS will remain compliant with the Data Security Standard (DSS) set forth by the Payment Card Industry for stand-alone dial-out terminals. No AHS data systems may store or transmit electronic cardholder data including the Primary Account Number (PAN), magnetic stripe data, expiration date, pin code/block, service code, card verification code, or card-validation code/value.

As a result of this policy, departments who engage in credit card processing shall provide and enact practices for:

- Annual training of personnel and raising security awareness relating to responsibilities according to the PCI DSS for those employees whose jobs entail processing such transactions.
- Monitoring of user activities to verify compliance with this policy and to detect actions that may be in violation of this policy.
- Reporting of all PCI DSS incidents, or suspected incidents to the designated AHS IT Incident Response team.
- Re-verifying and re-submitting the PCI DSS Self-Assessment Questionnaire Attestation of Compliance (SAQ) B annually.

- Verifying all paper including receipts generated as a product of point of sale transactions have the PAN masked.
- Prohibiting unencrypted email containing PAN data including but not limited to the subject and body of the messages.
- Limiting access to cardholder data to only those individuals whose jobs require such access.
- Avoiding paper storage of cardholder data whenever possible.
- Ensuring cardholder data remains physically secured and under strict control at all times.
- Cross-cut shredding all paper and receipts containing cardholder data after two years of storage.
- Ensuring departmental approval before the removal of cardholder data from the designated secured area in writing.
- Ensuring and documenting that partners and service providers who process transactions on behalf of the Agency adhere to the PCI DSS including an acknowledgement that the service provider is responsible for the security of the data the provider possesses.

COMPLIANCE:

It is the responsibility of the individual departments to ensure dissemination and review of this policy to all employees within their organizations and other associates as appropriate.

ENFORCEMENT:

The Office of the Secretary may initiate reviews, assessments or other means to ensure that policies, guidelines or standards are being followed.