

**MICHIGAN STATE UNIVERSITY
HEALTH INFORMATION TECHNOLOGY
POLICIES/PROCEDURES**

SUBJECT:	Credit Card Policy	NO: IS - 16
SCOPE:	HealthTeam, Faculty, Staff and Contract Users	Page 1 of 1
AUTHOR:	JJ Strieff, Linda Losik	INITIAL REVIEW REQUIRED BY:
FINAL APPROVAL: Jerry Aubert, CIO		
EFFECTIVE DATE: 10/2007		REVIEW DATE: 10/2008
KEYWORDS:		

POLICY

All payment information is considered to be both confidential and institutional data. Institutional data is defined both as data used in the normal course of business and the property of MSU. Confidential data is personal data that can be used in identity theft and related crimes and is required for normal business transactions.

Members of the Health Team and College staff may only have access to credit card information only with a specific “need to know” authorization as permitted and authorized by their job responsibilities.

Members of the Health Team and College staff may not save any payment information to the local computer or on any server, except where designated by the computer application such as QS1 or IDX.

If there is no approved application for billing, members of the Health Team and College staff must use the MSU web credit system.

Members of the Health Team and College staff may not store any credit card information on paper. All paper copies are to be given to the payee or shredded.

PROCEDURE

Health Team and College Staff

Officer Manager

HIT Security Officer and Network Manager

1. Swipe credit card or use credit card machine. Give paper printout to payee.
2. If there is no credit card swipe or credit card machine, use MSU web credit.
3. Report any intrusion or mishandling of credit card information to HIT Security Officer
4. HIT Security Officer will notify Network Manager and others according to the contact flowchart
5. HIT Security Officer will document all actions and maintain records for seven years.