Incident Response Plan – Merchant Sites
Credit Card Security Incident Procedures (Cardholder Data Compromise)

Overview – CMU departments that accept credit cards as a form of payment are responsible for the security of cardholder data per the Data Stewardship Policy. In the event that one or more credit cards have been compromised or appear to have been compromised, it is the responsibility of the department to inform the CMU Security Incident Response Team (CMU-SIRT) at security@cmich.edu or the Chief Information Security Officer (CISO) in the Office of Information Technology at 989-774-1474 or the Help Desk at 989-774-3662. The CMU-SIRT and CISO will investigate and escalate the matter appropriately. The CMU-SIRT will in turn contact Payroll and Travel Services and if necessary, CMU will use this same protocol to notify any affected individuals or other entities.

If your department has an actual or suspected breach, first you need to contain and limit your exposure. If you are using a terminal remove the phone cord from the terminal. DO NOT turn off the terminal.

Immediately contact the CMU Security Incident Response Team (CMU-SIRT) at security@cmich.edu or the Chief Information Security Officer (CISO) in the Office of Information Technology at 989-774-1474 or the Help Desk at 989-774-3662.

An assessment of the situation will be made. The following will be looked at…

1. Verify that no more credit card data is at risk.
2. The number of accounts at risk, and the type of data at risk (account numbers, expiration dates, cardholder names, CVV2 (3 or 4 digit code) and Track Data).
3. The date and time of the event.
4. The method of compromise.

The Merchant Account Manager must make themselves available for questions and will be responsible for helping the CMU Security Incident Response Team and the Chief Information Security Officer in the Office of Information Technology.