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

Overview – Binghamton University departments that accept credit cards as a form of payment are responsible for the security of cardholder data per Campus Policy 221. 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 BU Incident Response Team at pci-security-incident@binghamton.edu or the Chief Information Security Officer (CISO) at (607) 777-6198. The PCI Incident Response Team, including the CISO, will follow the procedures necessary to investigate and escalate the matter appropriately. The BU PCI IRT will in turn contact the Division of Business Affairs and if necessary, BU will use this same protocol to notify any affected individuals or other entities.

Immediately contact the BU Incident Response Team at pci-security-incident@binghamton.edu or the Chief Information Security Officer (CISO) at (607) 777-6198.

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.

If the suspected breach occurred over the internet, campus intranet, or with any computing technology device. The CISO must be notified immediately.

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 Director or Manager of the affected campus merchant department must make themselves available for questions and will be responsible for helping the BU PCI Incident Response Team and the CISO in the resolution process.