FSC Credit Card Security Incident Response Plan

To address credit cardholder security, the major card brands (Visa, MasterCard, Discover, American Express and JCB) jointly established the PCI Security Standards Council to administer the Payment Card Industry Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants create a security incident response team and document an incident response plan. The Farmingdale State College Credit Card Security Incident Response Team (Response Team) is comprised of the PCI Committee (see below for names and contact information). The Farmingdale State College security incident response plan is summarized as follows:

1. All incidents must be reported to a member of the Response Team.
2. That member of the team will report the incident to the entire Response Team.
3. The Response Team will investigate the incident and assist the compromised department in limiting the exposure of cardholder data.
4. The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc) as necessary.
5. The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

Farmingdale State College Credit Card Security Incident Response Team

Name	Telephone	Email
Justina Geremia	934-420-5365	Justina.geremia@farmingdale.edu
Jeff Borah	934-420-2661	Jeff.borah@farmingdale.edu
Margaret Steinhauer	934-420-5246	Margaret.steinhauer@farmingdale.edu
Keri Franklin	934-420-2424	Keri.franklin@farmingdale.edu
Dorothy Hughes	934-420-2166	Dorothy.hughes@farmingdale.edu

Incident Response Plan

An ‘incident’ is defined as a suspected or confirmed ‘data compromise’. A ‘data compromise’ is any situation where there has been unauthorized access to a system or network where cardholder data is collected, processed, stored or transmitted. A ‘data compromise’ can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.

In the event of a suspected or confirmed incident:

1. Do NOT touch or compromise any possible evidence. Do not shut off any computer or POS system.
2. Contact the Response Team. Make verbal contact with a team member, do not leave a voicemail. To report in incident after hours, contact University Police at 934-420-2111. When reporting an incident, include the following:
    a. Overview of incident, including date, time, and location of incident.
    b. Incident Type
        i. Computer Abuse
        ii. Malicious Code

        iii. Spam
        iv. Unauthorized Access/Use
        v. Breach of Physical Security (unlocked file cabinet, storage room etc.)
        vi. Possible tampering of POS machine
        vii. Other
    c. Intrusion Method
        i. Virus
        ii. Spyware/Malware
        iii. Stolen Password
        iv. Other
    d. Overview of data on the system? Was it sensitive?
    e. Explanation of discovery
    f. Action taken upon discovery
    g. Explanation of impact and impact on daily activities
    h. Any additional information
3. If the incident involves a payment station (PC used to process credit cards):
    a. Disconnect the network cable connecting the PC to the network jack. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.
4. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
5. Assist the Response Team as they investigate the incident.

Incident Response Team Procedures

The Response Team must be contacted by a department in the event of a system compromise or a suspected system compromise. After being notified of a compromise, the Response Team, along with other designated College staff from Information Technology, will implement their incident response plan to assist and augment the department's response plans.

In response to a system compromise, the Response Team and IT will:

1. Ensure compromised system is isolated on/from the network.
2. Gather, review and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection system logs.
3. Assist department in analysis of locally maintained system and other logs, as needed.
4. Conduct appropriate forensic analysis of compromised system.
5. If an incident of unauthorized access is confirmed and card holder data was potentially compromised, the Assistant Vice President for Finance and Controller will contact FSC's merchant service provider's customer service after informing the Executive Vice President for Administration and Finance and the Chief Financial Officer.
    a. The Response Team will contact the following payment card brands in the following manner for each card potentially breached;
        i. American Express guidelines
        ii. Discover Network guidelines
        iii. Visa guidelines
        iv. MasterCard guidelines

v. JCB guidelines

6. Assist law enforcement and card industry security personnel in investigative process.

The credit card companies have specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See Appendix A for these requirements.

Related Documents

American Express data incident guidelines

Discover Network data incident guidelines

Visa data incident guidelines

MasterCard data incident guidelines

JCB data incident guidelines