CREDIT CARD SECURITY INCIDENT RESPONSE PLAN

Synopsis:

To address credit cardholder security, the major card brands (Visa, MasterCard, Discover, American Express, and Diner's Club) 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. The guidelines require that merchants create a security incident response team and document an incident response plan. The Craven Community College Credit Card Security Incident Response Team (Response Team) is comprised of the following positions: Vice President of Administrative Services, Executive Director of Financial Services and Purchasing, Executive Director of Institutional Advancement, Dean of Technology & Facilities, Systems Administrator, and Craven County Sheriff Resource Officers for the New Bern and Havelock campuses.

Any employee of Craven Community College who becomes aware of an Incident (as defined herein), should contact the Craven Community College Credit Card Security Incident Response Team, which, along with other designated college staff, will implement the Incident Response Plan to address the Incident.

Craven Community College Credit Card Security Incident Response Team

Position Title	Current Employee	Office Phone Number	Mobile Phone Number	Email	Role
VP of Administrative Services	Page Varnell	252.672.1751	252.876.3354	jonesp@cravencc.edu	Administration
Executive Director, Financial Services and Purchasing	Cindy Patterson	252.638.7304	252.876.7136	pattersonc@cravencc.edu	Finance Officer
Dean of Technology	Julia Hamilton	252.638.7317	252.670.0123	hamiltonj@cravencc.edu	Technology Officer
Director of Communications	Craig Ramey	252.638.7210	250.259.0309	rameyc@cravencc.edu	Public Information Officer
Systems Administrator	Deborah Joyner	252.638.7264	252.229.7654 or 252.876.2133	joynerd@cravencc.edu	Subject Matter Expert
C.C. Sheriff Resource Officer (New Bern)	Anthony DeJesus	252.638.7261	252.626.3998	dejesusa@cravencc.edu	NB Law Enforcement
C.C. Sheriff Resource Officer (Havelock)	Scott Gaskins	252.444.3343	252.229.7964	gaskinsmi@cravencc.edu	Havelock Law Enforcement

Incident Response Team Coordinators

Position Title	Current Employee	Office Phone Number	Mobile Phone Number	Email
Controller	Christine Hurst	252.637.5740	252.671.9086	hurstc@cravencc.edu
Director, Networking & Information Security	Shawn Toderick	252.639.9307	336.776.7567	todericks@cravencc.edu
Network and Information Security Administrator	Jonathan Irwin	252.672.7508	252.259.0191	irwinj@cravencc.edu
Information Security Support	Elaine Rouse	252.638.7372	252.626.8360	rousee@cravencc.edu
Director of Student Accounts	Kisha Simpson	252.638.7203	252.259.5366	bectonk@cravencc.edu
Security Operations Coordinator	Jackie Thomas	252.638.7400		thomasj@cravencc.edu
Information Technology Support	Doyle Owings	252.447.1775	252.617.1085	owingsd@cravencc.edu

In addition, each of the following persons may provide supporting roles during the incident response: Information Systems Specialists, and Chief Campus Security Officer.

Any incidents that occur after normal working hours should be reported to Security at 252-638-7261.

Definition of "Incident"

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

Incident Response Plan

In the event of an Incident:

1. All incidents must be immediately reported upon discovery to the supervisor of the reporting person and to the entire Response Team.
    a. If the incident involves a payment device (such as a POS register or PC used to process credit cards), the reporting person should be instructed as follows:
        i. Do not turn off the unit.
        ii. Disconnect the network cable from the back of the POS unit.
        iii. Place sign on PC to not power down.
        iv. Await further instruction from the Response Team.
        v. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.

b. If any employee of the College suspects loss or theft of any materials containing cardholder data, the employee must immediately notify his or her immediate supervisor and the Credit Card Security Incident Response Team via breach@cravencc.edu. The email should be conducted from a separate workstation not the one that has been compromised.

c. All employees of Craven Community College shall fully comply with the Response Team, and assist the Response Team as requested, as they investigate the incident.

d. The Response Team will take all reasonable steps as soon as practicable to limit the exposure of cardholder data and assist the compromised department. Such steps may include ensuring the compromised system is isolated from the network, if appropriate.

e. A sweep will be commenced of all POS computers on both campuses at this point to make sure the breach has not occurred any other POS computers.

2. <u>Evidence Handling</u>

Handling of evidence is imperative in the case of legal action. Upon initiation of an incident response, a designated chain of custody and evidence handling to be performed by the Craven County Sheriff's Resource Officer.

a. Least privilege will be used judiciously, any personnel outside of the chain of custody shall not have access, even if the person requesting is part of the incident response team.

b. Evidence will be turned over to law enforcements if the incident requires us to do so.

c. Information shall be recorded in accordance with Statewide Information Security Manual, dated 7/23/2014, Section 130101, and shall be reported at https://it.nc.gov/cybersecurity-situation-report.

3. The Response Team will perform a reasonable investigation of the incident under the circumstances. The investigation may include the following:

a. Gathering, reviewing and analyzing all centrally maintained system, firewall, file integrity and intrusion detection/protection system logs.

b. Assisting department in analysis of locally maintained system and other logs, as needed.

c. Retaining electronic files and hardware for possible forensic research.

d. All information pertaining to this breach shall be kept within the team and parties that will help resolve the issue. The breach shall not be disclosed to outside parties without permission from the team.

4. If it is reasonably believed that misuse of cardholder data was or is likely, the following steps shall be taken by the Response Team:

a. The Dean of Technology and Facility Services will contact Craven Community College's card payment processing bank(s) after informing the Executive Director of Financial Services and the Vice President of Administrative Services.

b. For incidents involving Student Accounts – New Bern and Havelock, the Response Team will contact Official Payments at ClientServices@OfficialPayments.com or call 866-352-5002.

c. For incidents involving Public Radio East, contact Sun Trust/Intellipay, Inc. at 801-578-9020.

d. For incidents involving the Craven Community College Foundation, contact Blackbaud at 800-443-9441

e. The Response Team should contact the appropriate governmental and law enforcement authorities. (Contact information is provided on Exhibit A.) The Response Team and other employees should, as requested:

i. Make information available to appropriate law enforcement personnel; and

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

5. The major credit card networks have specific requirements the Response Team should observe in reporting Incidents. (See Exhibit B for these requirements.)

6. The Response Team will take all steps necessary to comply with security breach response requirements of N.C.G.S § 75-65 pursuant to N.C.G.S. § 132-1.10(c1), which shall include the following:

a. Providing notice to the affected person that there has been a security breach without unreasonable delay, consistent with the legitimate needs of law enforcement, to the extent required by law; and

b. Providing notice without unreasonable delay to the Consumer Protection Division of the North Carolina Attorney General's Office, if required, of the nature of the breach, the number of customers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.

7. The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

Exhibit A

FBI Charlotte
7915 Microsoft Way
Charlotte, NC 28273
Charlotte.fbi.gov
(704) 672-6100

ICANN computer Incident Response Team
4676 Admiralty Way, Suite 330
Marina Del Rey, CA 90292
310-823-9358

North Carolina Department of Justice

Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6400 - Fax: (919) 716-6750

Legal Services Division
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6400 - Fax: (919) 716-6750

State Bureau of Investigation
Post Office Box 29500
Raleigh, NC 27626
Telephone: (919) 662-4509 - Fax: (919) 716-6750

New Bern Police Department
Sgt. Paul D. Brown
brownp@newbernpd.org
252.672.4247
252.349.3715 (mobile)

Exhibit B

MasterCard – Responding to a Breach
Follow the steps set forth in the
https://www.mastercard.us/en-us/merchants/safety-security/suspect-fraud.html

Visa – Responding to a Breach
Follow the steps set forth in the resource:
https://usa.visa.com/dam/VCOM/global/support-legal/documents/responding-to-a-data-breach.pdf

American Express – Responding to a Breach
See Merchant Information – In Case of Breach at :
https://www260.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US&tabbed=breach

Discover Card Specific Steps
1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers 4. Obtain additional specific requirements from Discover Card