Communication Plan for Security Breach Policy for Credit Card information and Other "Identifying Information".

Purpose

To provide the campus community guidelines on what to do and which departments that must be contacted if a department experiences or suspects a security breach that involves credit card information and/or identifying information. Credit card information and identifying information can be both electronic and non-electronic information

---

Policy

Within 24 hours of a known or suspected security breach, the following departments must be notified:

1. Department Supervisor & University Controller
2. University Credit Card Compliance Committee
3. IT Network Security Officer - if breach involves electronic data
4. University Police-

Departments must report any actual or suspected security incident in which cardholder information may have been compromised. The incident should be reported immediately to the Credit Card Compliance Committee and the University Controller. A written report must be completed that documents and describes the incident. If the incident involves the loss or suspected compromise of stored or processed electronic data, the incident must also be reported to the IT Security Officer. This must be done immediately. The University's Compliance Committee must report all breaches to the State Controller's Office within 24 hours of the detection.

Credit Card Compliance Committee

Denise Foutz, Special Projects	262.6119
Oscar Knight, IT Network Security Officer	262.6946
Karen Main, Internal Audits	262.2281

Credit Card Information

Credit Card sensitive information includes the following data or the combination of such data :

1. Credit Card number & expiration date
2. Name and Billing information
3. CVV2: 3-digit value located on the back of the card.
4. Any information located on the magnetic stripe.

Identifying Information

Identity theft (as defined by § 14-113.20)

(a) A person who knowingly obtains, possesses, or uses identifying information of another person, living or dead, with the intent to fraudulently represent that the person is the other person for the purposes of making financial or credit transactions in the other person's name, to obtain anything of value, benefit, or advantage, or for the purpose of avoiding legal consequences is guilty of a felony punishable as provided in G.S. 14-113.22(a).

(b) The term "identifying information" as used in this Article includes the following:

(1) Social security or employer taxpayer identification numbers.
(2) Drivers license, State identification card, or passport numbers.
(3) Checking account numbers.
(4) Savings account numbers.
(5) Credit card numbers.
(6) Debit card numbers.
(7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
(8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
(9) Digital signatures.
(10) Any other numbers or information that can be used to access a person's financial resources.
(11) Biometric data.
(12) Fingerprints.
(13) Passwords.
(14) Parent's legal surname prior to marriage.

Statutory Requirements

1. Cash Management Law, as specified in G.S. 147-86.10

2. G.S. 14-113.20 defines the “identifying information” that is subject to the Identity Theft Protection Act, which includes but is not limited to, “credit card numbers” and “debit card numbers.”

3. G.S. 114-15.1 requires that the State Bureau of Investigation receive written notification of any information or evidence of "damage of, theft from, or theft of, or misuse of, any state-owned personal property." This reporting requirement includes reports of a security threat or breach of the state's information systems.

4. G.S. 147-33.113 requires the head of each State agency to

cooperate with the State Chief Information Officer in the discharge of his or her duties by, “Providing the full details of the agency's information technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation.”

5. G.S. 147-64.6(c)(18) requires the State Auditor, after consultation and in coordination with the State Chief Information Officer, to assess, confirm, and report on the security practices of information technology systems.