NC OSC Policy 500.10

Merchant Cards Security Incident Plan

Policy Area**: eCommerce**	Effective Date: **02/01/2007**
Policy Sub Area**: NA**	Last Revision Date**: NA**
Authority: **G.S. 14-113.20; G.S. 75-61(14); G.S. 114-15.1; G.S. 147-33.113; and G.S. 147-64.6(c)(18)**	Policy Owner/Division**: Statewide Accounting**

Policy

All participants in the State Controller's Master Services Agreement for Merchant Card Services, as well as State agencies engaging in separate arrangements, are to devise a security incident response plan that incorporates the requirements of the Payment Card Industry Security Council. For those State agencies falling under the purview of The State Chief Information Officer, the incident response requirements defined by the Office of Information Technology Services (ITS) should also be incorporated.

- The agency's incident response plan must include the requirements of the Payment Card Industry Data Security Standard (PCI DSS):
    - Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies.
    - Test the plan at least annually.
    - Designate specific personnel to be available on a 24/7 basis to respond to alerts.
    - Provide appropriate training to staff with security breach response responsibilities.
    - Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.
    - Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
- The agency's plan must include the notification requirements of the various State governing agencies as applicable.
    - In all cases, notify the Office of the State Controller (OSC) within 24 hours of a known or suspected security breach.
    - If the agency falls under the purview of The State Chief Information Officer), and if the incident involves technology systems, notify the ITS Information Security Office, within 24 hours of a known or suspected security breach, and in accordance with the procedures specified by the Statewide Incident Management Plan.
- In accordance with the card associations rules, each card association and proprietary card

company is to be notified whenever a security breach is known to have occurred or is suspected to have occurred. Notification is to be made through the merchant card processor. Requirements generally require a notification to be made within a specific timeframe, and an incident report to be submitted within a specific time frame:

- If the agency is a participant in the State Controller's Master Services Agreement for Merchant Card Services, the participant is to consult first with the OSC, and the OSC shall make the appropriated notifications on the agency's behalf, or advise otherwise.
- If the agency is not a participant in the State Controller's Master Services Agreement for Merchant Card Services, the agency shall consult with both the OSC and the merchant processor that it has contracted directly with regarding appropriate notifications.

- When reporting a security incident to the OSC, all pertinent details of the incident are to be provided to assist the OSC in making an assessment of the seriousness and extent of the incident. Any credit card data provided to the OSC as part of the assessment process shall be transmitted in a secure encrypted manner.
- Whenever a press release regarding the occurrence of a security breach is warranted, the OSC should be consulted first, in order to coordinate the timing of the release with any other notifications that may be required.
- In cases where a security incident is required to be reported to the card associations, the card associations may require a forensic investigation to be performed by a Qualified Security Accessor (QSA). For those agencies that are participants under the State Controller's Master Services Agreement, the participant may elect to use a QSA that the OSC may have a contract with to provide such services. Agencies are responsible for the costs of any forensic services provided.

Procedures

NA

Accounting Guidance

IT Security Office-- https://incident.its.state.nc.us/

PCI Security Standards Council-- https://www.pcisecuritystandards.org

Related Documents (Memos/Forms)

NA

Revision History

Date	Description
NA	