THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Responsible University Officer
Chief Information Officer

Responsible Office
Information Security Office

PCI DSS INCIDENT RESPONSE PLAN

Incident Response Plan for PCI DSS Incidents

The Incident Management Policy requires “every faculty member, staff member, student, temporary employee, contractor, outside vendor, and visitor to campus (AKA User) who has access to University-owned or managed information through computing systems, devices, or physical files” to “report Information Security Incidents” per the procedures defined. As defined in the Incident Management Policy, sensitive information includes “card holder data,” as defined by the Payment Card Industry (PCI) Data Security Standards.

As stated in the Incident Management Policy, Information Technology Services, Information Security Office (ITS, ISO), in conjunction with the Office of University Counsel and the affected University department, shall direct the incident response and investigation. The ITS, Information Security Office, the Office of University Counsel, and the affected University department will coordinate on business recovery procedures, business continuity procedures, and data back-up processes, as appropriate. Coordination of activities may include the Department of Public Safety (DPS) when physical files are involved.

Specific incident response procedures are defined at the “Incident Management Procedures” link listed in the “Incident Management Policy” and other locations consistent with availability to appropriate personnel. Communication and contact strategies in the event of an “Information Security Incident” are defined in the “Incident Reporting” section of the Incident Management Procedures, and other locations consistent with availability to appropriate personnel. The ITS Information Security Office will coordinate with the Office of University Counsel, as appropriate, when the notification of the payment brands may be necessary. The Office of University Counsel is responsible for the ongoing analysis of legal requirements for reporting compromises.

Specific procedures are documented in protected help.unc.edu documents and other locations specific to the groups with a business need to access the documents.

As a part of the incident response process, consultation of incident response procedures proposed by the payment brands may be required:

- American Express Data Security Operating Policy[1]

- MasterCard Account Data Compromise User Guide[2]
- Visa – Responding to a Data Breach[3]
- Visa – What To Do If Compromised[4]

[1] https://www209.americanexpress.com/merchant/services/en_US/data-security
[2] https://www.mastercard.us/content/dam/mccom/en-us/documents/account-data-compromise-manual.pdf
[3] https://usa.visa.com/support/small-business/data-security.html/
[4] https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

Related Regulations, Statutes, and Related Policies

- Payment Card Industry Data Security Standard (PCI DSS)
- UNC-Chapel Hill, Incident Management Policy
- UNC-Chapel Hill, Incident Management Procedures
- UNC-Chapel Hill, Payment Card Industry, incident management specific procedures can be found in the Information Security Office wiki and on the School of Medicine/ISO share

Document History

- Effective Date: 10/01/14
- Review Date: 9/16/2014, 10/13/2015 (CISO), 10/17/2016 (CISO)