George Mason University	*University Standard* **Incident Response Plan for PCI DSS incidents**
Version 1.0	*Date of last revision: 04/26/16*

The purpose of this standard is to define requirements for responding to a cyber security incident involving credit card holder data.

User Requirements:

University Policy 1305: *Reporting Electronic Security Incidents* requires every faculty member, staff member, student, temporary employee, contractor, outside vendor, and visitor to campus who has access to University-owned or managed information through University-provided or personal computing systems, devices, or physical or electronic files to report Information Security Incidents. As defined in University Policy 1114: *Data Stewardship*, sensitive information includes "payment card numbers associated with a personal identifier," as defined by the Payment Card Industry Data Security Standards (PCI DSS).

As stated in University Policy 1305, Information Technology Services and the Information Technology Security Office, in conjunction with the Office of University Counsel and the affected University department, shall direct the incident response and investigation. The ITS, the Information Technology 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.

Specific procedures are defined in University Policy 1305. The policy can be found here: http://universitypolicy.gmu.edu/policies/reporting-electronic-security-incidents. Communication and contact strategies in the event of an information security incident are also defined in the "IV. RESPONSIBILITIES" and "V. DATA BREACH NOTIFICATION RESPONSIBILITIES" sections of University Policy 1305. 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.

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] http://www.mastercard.com/us/merchant/pdf/ADC_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