Appendix C – PCI Incident Response Plan

All actual or suspected breaches must be reported to the ISO by calling (213) 740-5555, which is a call center operated 24 hours a day, 7 days a week. Upon notification, the ISO and Office of Compliance are responsible for investigating and coordinating with necessary members of the university community to ensure PCI requirements are met as described below. Departments may not conduct their own investigation without first consulting and coordinating with the ISO.

The ISO will:
- Determine whether an incident has occurred;
- Analyze and correlate initial information reported to the ISO;
- Gather research based on other means such as technical capabilities;
- If an incident is believed to have occurred, begin documenting the investigation and continue gathering evidence; and
- Ensure appropriate containment of the incident using the most appropriate options.

The ISO, in conjunction with the Office of Compliance, will:
- Prioritize handling the incident based on risk and impact to the organization; and
- Convene the incident response team described in this PCI policy, as applicable.

The Office of Compliance will:
- Engage IDExperts, as applicable, to facilitate call center and other consumer services;
- Conduct a legal analysis in coordination with Office of the General Counsel to determine whether a breach has occurred as defined under law or regulations, including California Civil Code Section 1798.82; and
- Manage the breach notification process required under law or regulation.

The ISO and Office of Compliance will:
- Consult with the incident response team on a regular basis regarding the incident and status of response;
- Report to other units within USC and senior management based on the analysis of legal requirements and criticality of systems’ information within USC’s Business Continuity/Disaster Recovery Plans; and
- Implement appropriate corrective action, including administrative, physical and technical safeguards as recommended by the incident response team and approved by senior management.

The Office of Compliance will manage the process to report to appropriate parties in coordination with the ISO and incident response team:
- To the credit card issuing organizations to fulfill their PCI requirements:
  - **MasterCard**
  - **Visa**
    - [http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html](http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html)
  - **Discover**
http://www.discovernetwork.com/index.html - call fraud department at (800) 347-6634

**American Express**

- To local and federal law enforcement as deemed appropriate by the incident response team;
- To impacted individuals;
- To applicable state and federal regulatory agencies as required by law;
- To Human Resources to determine appropriate disciplinary action, as applicable;
- Implement additional monitoring to look for future related activity, if appropriate; and
- Prepare investigation report, as applicable.

The incident response team will debrief from incident and implement any lessons learned.