UNIVERSITY OF CAMBRIDGE
Finance Division

PCI DSS Compliance Policy

The University of Cambridge PCI DSS Compliance policy is:

- The University will undertake a PCI Compliance review on an annual basis.
- If any member of staff identifies that this policy is compromised or is at risk of compromise then he/she must report the matter immediately to the PCI Compliance Officer. The PCI Compliance Officer will then invoke the Incident Report Plan. The PCI Compliance Officer can be contacted at: PCIcompliance@admin.cam.ac.uk
- All staff who handle either "customer present" or "customer not present" card transactions in any form shall undertake PCI Compliance training on an annual basis.
- All "customer present" card transactions must take place using a PCI compliant electronic point of sale system.
- Where an electronic point of sale system is hired for an ad-hoc event, this must be hired directly from Barclaycard to ensure it is fully PCI Compliant.
- Wherever possible "customer not present" card transactions should be processed using the University's online store (WPM e-Sales) system.
- Where a personal computer or similar is used to access systems to process card transactions, the personal computer or similar must be an asset of the University. A personal computer owned by an individual must not be used.
- Under no circumstances should card and/or cardholder details be stored or transmitted electronically (other than through the University's online store). This includes emailing, instant messaging, chat and scanning of paper copies.
- If there is a valid requirement to scan paper copies containing card transaction details, the card details must be obliterated using an indelible marker pen before scanning.
- Where paper copies containing card transaction details need to be retained for a valid reason, for example chargebacks, they must be retained in a secure, locked cabinet or room at all times.
- The retention period for all paper copies containing card transaction details is:
  - File by date of transaction
  - Merchant copies should be kept for a minimum of 6 months (this is the time limit with which chargebacks can be registered)
  - Beyond this, copies should be kept for a further 12 months

  (i.e. TOTAL storage time equals 18 months from date of transaction)
- All other paper copies containing card transaction details must be destroyed (cross shredded) immediately after use.

- The University will carry out penetration testing at least annually on the University network and the results will be notified to the PCI Compliance Officer.

- The University will use and regularly update anti-virus software to protect the University network and its personal computers.

- The University will contract an approved external supplier to carry out quarterly vulnerability scans of the relevant University IP addresses and the results will be notified to the PCI Compliance Officer.

- All individuals handling card data are expected to comply with:

    - Information Strategy and services syndicate policy - Use and Misues of Computing Facilities http://www.ucs.cam.ac.uk/isss/rules/guidelines.html
    - Human Resources Divison - Acceptable use of computer facilities, email and the internet.
      http://www.admin.cam.ac.uk/offices/hr/policy/computer.html
    - Information Data Security policy
      http://www.admin.cam.ac.uk/reporter/2001-02/weekly/5895/8.html