Information Security Policy

London Brookes College ('LBC')

(Company Name)

25 August 2015

(Date)

Contents

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2. Information Security Policy

LBC handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

LBC commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling Sensitive cardholder data should ensure

- Handle Company and cardholder information in a manner that fits with their sensitivity;
- Limit personal use of LBC information and telecommunication systems and ensure it doesn't interfere with your job performance;
- LBC reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;

- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to LBC's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. LBC will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of LBC, unless posting is in the course of business duties.

- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non compliance.

5. Protect Stored Data

All sensitive cardholder data stored and handled by LBC and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the company for business reasons must be discarded in a secure and irrecoverable manner.

If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance

6. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level:

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to LBC if disclosed or modified. **Confidential data includes cardholder data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure;
- **Public data** is information that may be freely disseminated.

7. Access to the sensitive cardholder data:

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum of the first 6 and the last 4

digits of the cardholder data.

- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
- LBC will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- LBC will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- The company will have a process in place to monitor the PCI DSS compliance status of the Service provider.

8. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on LBC sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

9. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or by any modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption,SSL,TLS,IPSEC etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by LBC, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- LBC will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- LBC will have documented procedures for the destruction of electronic media. These will require:
    - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.

- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A)
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the company.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

12. Security Management / Incident Response Plan

Employees of the company will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within the company and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Incident Response Plan

1. In the event of a suspected security breach, alert the information security officer or your line manager immediately.
2. The security officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

13. Network security

- Stateful Firewall technology must be implemented where the Internet enters the LBC Card network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.

- All inbound network traffic to the campus is blocked by default, unless explicitly allowed and the restrictions have to be documented.

- All outbound traffic has to be authorized by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented

- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.

- The firewall rules will be reviewed on a six months basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base

- LBC have to quarantine wireless users into a DMZ, where they were authenticated and firewalled as if they were coming in from the Internet.

- No direct connections from Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall.

Rules	Source IP	Destination IP	Action

14. System and Password Policy

All users, including contractors and vendors with access to LBC systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into the LBC network and all unnecessary services have to be disabled.

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.

- Where SNMP is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.

- For non-console administerative access prevent the usage of insecure technologies like telnet etc. and use appropriate technologies like ssh,vpn,ssl etc and strong cryptography.
- Administrator access to web based management interfaces is encrypted using strong cryptography.

15. Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by LBC. The preferred application to use is LBC Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus

16. Patch Management Policy

- All Workstations, servers, software, system components etc. owned by LBC must have up-to-date system security patches installed to protect the asset from known vulnerabilities.

- Where ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from the respective vendor.

- Any exceptions to this process have to be documented.

17. Remote Access policy

- It is the responsibility of LBC employees, contractors, vendors and agents with remote access privileges to LBC's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to LBC.

- Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.

- All hosts that are connected to LBC internal networks via remote access technologies will be monitored on a regular basis.

- All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.

- Vendor accounts with access to LBC network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

18. Wireless Policy

- Installation or use of any wireless device or wireless network intended to be used to connect to any of the LBC networks or environments is prohibited.

- Usage of appropriate testing using tools like net stumbler, kismet etc. must be performed on a quarterly basis to ensure that:
  - no wireless devices or networks have been deployed;
  - Any devices which support wireless communication remain disabled or decommissioned.

- If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the LBC has the authorisation to stop, cease, shut down, and remove the offending device immediately.

  If the need arises to use wireless technology it should be approved by LBC and the following wireless standards have to be adhered to:

  1. Default SNMP community strings and passwords, passphrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves the company.

  2. The firmware on the wireless devices has to be updated accordingly as per vendors release schedule

19. Vulnerability Management Policy

- As part of the PCI-DSS Compliance requirements, LBC will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as

new system component installations, changes in network topology, firewall rule modifications, product upgrades).

- Quarterly internal vulnerability scans must be performed by LBC by internal staff or a 3rd party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.

- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by the company's internal staff. The scan process should include re-scans until passing results are obtained.

20. Roles and Responsibilities

- Chief Security Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:

- creating and distributing security policies and procedures
- monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel
- creating and distributing security incident response and escalation procedures that include:
- maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)

- The Information Technology Office (or equivalent) shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).

- System and Application Administrators shall:

- monitor and analyse security alerts and information and distribute to appropriate personnel
- administer user accounts and manage authentication
- monitor and control all access to data
- maintain a list of service providers
- ensure there is a process for engaging service providers including proper due diligence prior to engagement
- maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation

- The Human Resources Office (or equivalent) is responsible for tracking employee participation in the security awareness program, including:

- facilitating participation upon hire and at least annually

- ensuring that employees acknowledge in writing at least annually that they have read and understand the company's information security policy

- General Counsel (or equivalent) will ensure that for service providers with whom cardholder information is shared:

- written contracts require adherence to PCI-DSS by the service provider
- written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider

21. Transfer of sensitive Information Policy

- All third-party companies providing critical services to LBC must provide an agreed Service Level Agreement.

- All third-party companies providing hosting facilities must comply with the Company's Physical Security and Access Control Policy.

- All third-party companies which have access to Card Holder information must

    1. Adhere to the PCI DSS security requirements.

    2. Acknowledge their responsibility for securing the Card Holder data.

    3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.

    4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.

    5. Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.

22. User Access Management:

- Access to LBC is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.

- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to cardholder data
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

  Name of person making request:

  Job title of the newcomers and workgroup:

  Start date:

  Services required (default services are: MS Outlook, MS Office and Internet access):

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all LBC systems is provided by IT and can only be started after proper procedures are completed.

- As soon as an individual leaves the LBC employment, all his/her system logons must be revoked.

- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

Checked on 4th August 2021 by Cillian Logue