Data Security and Protection Procedures

Document Title	Data Security and Protection Procedures
Document Owner	IT Department
Approved By	Information Steering Committee
Date Approved	02 October 2023
Date of Review	02 October 2024
Document Version	1.1

Objective

The purpose of this document is to establish comprehensive data security and protection procedures for London Campus of Higher Studies to ensure the confidentiality, integrity, and availability of sensitive information. These procedures are designed to safeguard student, staff, and institutional data against unauthorized access, disclosure, alteration, and destruction.

1. Data Classification: All data must be classified based on its sensitivity and importance. Classifications may include Public, Internal, Confidential, and Restricted. Each classification will have associated security measures.

2. Access Control:

a. User Authentication:

Strong passwords must be enforced for all user accounts. Implement multi-factor authentication (MFA) for access to sensitive systems and data. Regularly review and update user access credentials.

b. User Authorization:

Grant access permissions based on the principle of least privilege. Conduct regular access reviews to ensure users have the necessary permissions for their roles. Immediately revoke access for individuals who no longer require it.

3. Physical Security:

a. Secure Facilities:

Restrict physical access to data centers and server rooms. Implement surveillance and access control systems for restricted areas. Regularly review and update physical security measures.

b. Device Security:

Encrypt all portable devices (laptops, tablets, etc.) to protect data in case of loss or theft. Install and update antivirus software on all devices.

4. Network Security:

a. Firewalls and Intrusion Prevention Systems (IPS): Deploy firewalls and IPS to monitor and control network traffic. Regularly update firewall rules to reflect changes in the network environment.

b. Secure Wi-Fi:

Use strong encryption protocols for wireless networks. Change default credentials for Wi-Fi routers. Regularly update Wi-Fi passwords.

5. Data Encryption: Encrypt sensitive data during transmission and storage to prevent unauthorized access. Implement encryption protocols such as SSL/TLS for data in transit and encryption algorithms for data at rest.

6. Data Backups: Regularly back up critical data to ensure data recovery in case of system failures, data corruption, or other disasters. Store backup copies in secure and offsite locations.

7. Incident Response: Develop and implement an incident response plan to address security incidents promptly. This plan should include procedures for identifying, reporting, and responding to security breaches.

8. Security Awareness Training: Conduct regular security awareness training for all staff and students to educate them on security best practices, phishing awareness, and the importance of data protection.

9. Compliance and Auditing: Ensure compliance with relevant data protection laws and regulations. Conduct regular security audits and assessments to identify and address potential vulnerabilities.

10. Data Disposal: Establish procedures for the secure disposal of data, including physical documents and electronic media. Use secure deletion methods for digital data.

11. Vendor Management: Evaluate and monitor third-party vendors for their data security practices. Ensure that vendors handling sensitive information adhere to the same security standards as the institution.

12. Continuous Improvement: Regularly review and update data security procedures based on emerging threats, technological advancements, and changes in the institutional environment.

Conclusion: Adherence to these data security and protection procedures is essential to maintain the trust of students, staff, and stakeholders. All members of London Campus of Higher Studies are responsible for implementing and following these procedures to safeguard the institution's data assets effectively.

This document should be regularly reviewed, updated, and communicated to all relevant stakeholders to ensure ongoing compliance and effectiveness.

HOW CAN YOU CONTACT US ABOUT THIS POLICY?

If you have questions or comments about this policy, email **Mr. Arshmaan Talib** at **Admin@lchs.org.uk** or by post to:

London Campus of Higher Studies

Operations/ Policy

Southbridge
House,
Southbridge
Palace, London.
CR0 4HA

Hamzah Tariq Khan *Hamza Khan*	Muhammad Saqib Sohail *Saqib Sohail*
Director Admin / Operation	**Director Academic Affairs**
02 October 2024	02 October 2024