Information Security

Title: Information Security Policy

Number: ISM001 v.1.6 (27/05/2009)

Description: London School of Economics & Political Science Information Security Policy

Introduction

1. The confidentiality, integrity and availability of information, in all its forms, are critical to the continued success of the staff and students of the LSE, as well as the institution itself. Failure to secure information increases the risk of financial and reputational losses from which it may be difficult to recover.

Purpose

2. This information security policy provides the overall framework within which the security of information will be maintained and promoted across the LSE. Specific, subsidiary information security regulations and procedures shall be considered part of this information security policy and shall have equal importance.

3. It also defines relevant roles and responsibilities that relate to the implementation of this policy.

Scope

4. This policy is applicable to, and will be communicated to, all staff, students, other members of the School and third parties who interact with the information held by the LSE in all its forms and its related information systems. This includes, but is not limited to, any systems or data attached to the LSE computer or telephone networks, systems supplied by the LSE or communications sent to or from the LSE.

5. Information, in this context, is defined as knowledge that has value to LSE and is in a form that is accessible to others, either physically or electronically.

Policy Statement

6. The LSE is committed to the security of its information and information systems:
    a. Maintaining confidentiality: only allowing authorised access to information;
    b. Ensuring integrity: preventing unauthorised modification of information;
    c. Assuring availability: critical information must be accessible when it is needed;
    d. Ensuring legal compliance: making sure that the LSE is compliant with all relevant legislation.

7. This will be achieved by implementing additional, subsidiary information security regulations relating to specific areas. Appropriate controls will be implemented to endeavour to ensure the confidentiality, integrity and availability of information from accidental and deliberate acts. These include:
    a. The Conditions of Use for IT Services
    b. Information Security Infrastructure
    c. Information Security Operations
    d. Information Handling
    e. Information Systems User Management
    f. Information Systems Planning
    g. Information Systems Management
    h. Network Management
    i. Software Management
    j. Information Security of Mobile Computing and Tele-working
    k. Information Systems Business Continuity Planning
    l. Cryptography
    m. Information Systems Compliance

8. This policy, and its subsidiaries, shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations by the Information Security Group and an auditor external to IT Services. Additional regulations may be created to cover specific areas.

9. To determine the appropriate levels of security measures applied to information systems, a process of risk assessment and periodic reviews shall be carried out for each system to identify the probability and impact of security failures by the person responsible for the information contained within that system.

10. An information security steering group, comprising management representatives from all relevant parts of the organisation, shall devise and coordinate the implementation of information security controls and approve subsidiary policies.

Roles and responsibilities of the School

11. The Director has the overall responsibility for the implementation of this policy in the School, with day-to-day responsibility delegated to the Information Security Manager.

12. Managers of departments who run systems have the responsibility to implement controls and identify risks with their individual systems, in accordance with the advice of specialist risk sections within the School.

13. The Librarian and Director of IT Services is responsible for ensuring that appropriate security measures are put in place for centrally managed IT systems.

14. The Information Security Manager is responsible for this and subsequent information security policies and will provide specialist advice throughout the School on information security issues.

15. The Head of Security is responsible for physical aspects of security and will provide specialist advice throughout the LSE on physical security issues.

16. All staff, students, visitors and third parties related to the School must handle information in accordance with this policy and any relevant local legislation, either in the UK, EU or where ever the information or data are being held or processed.

17. The implementation of this policy shall be reviewed independently by an agreed party at regular intervals agreed by Internal Audit and IT Services.

18. The School will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

Reporting

19. Any actual or suspected breach in information security must be reported to the Information Security Manager in a timely manner, who will take appropriate action and inform the relevant authorities.

Disciplinary Procedure

20. Failure to comply with this policy, or its subsidiary regulations, may result in disciplinary action.

Stephan Freeman – May 2009