General Osteopathic Council – Information Security Policy

Introduction

1. Data stored in information systems represents an extremely valuable asset. The General Osteopathic Council (GOsC) recognises that data stored by it on information systems is fundamental to its statutory role of regulating osteopaths in the United Kingdom. The GOsC has a responsibility to its stakeholders to ensure that these systems are developed, operated and maintained in a safe and secure fashion. Increased activity in transmitting information across networks of computers and between third party organisations, makes data extremely vulnerable to accidental or deliberate, unauthorised modification or disclosure. The consequences of information security failures can be costly, in both financial and reputational terms, and rectification can be extremely time-consuming.

2. This outline Information Security Policy sets out appropriate security objectives and responsibilities through which the GOsC will facilitate the secure and reliable flow of information, both within the GOsC and in external communications. The GOsC will use the twelve major sections of the ISO/IEC 27002 (best practice recommendations on information security management) as a framework to ensure that it manages adherence to this policy in the best possible manner.

Objectives

3. The objective of this policy is to ensure that all information and information systems upon which the GOsC depends are adequately protected to the appropriate level. This is supported by the Senior Management Team's (SMT) commitment to:

    a. view information security as a business critical issue;
    b. develop a culture of information security awareness;
    c. use established methods for risk assessment, management and acceptance;
    d. implement information security controls which are proportionate to risk;
    e. requiring individual accountability for compliance with information security policies and supporting procedures.

Scope

4. The scope of this policy extends to all information in all its forms handled by GOsC employees, including temporary staff, as well as contractors, non-executive members (Council, committees etc), GOsC associates, and agents. The information may be on paper, stored electronically or held on film, microfiche or other media. It includes data, text, pictures, audio and video. It covers information transmitted by post, by electronic means and by oral communication, including telephone and voicemail.

5. This policy applies throughout the lifecycle of the information, from creation through storage and use, to disposal. Appropriate protection is required for all forms of information, to ensure business continuity and to avoid breaches of the law, and to meet statutory, regulatory or contractual obligations. This also includes all GOsC owned/licensed data and software, be they loaded on GOsC or privately/externally owned systems, and to all data and software provided to the GOsC, by sponsors or external agencies.

6. The scope of this policy extends to all processing and storage systems used in support of the GOsC's operational activities to store, process and send and receive information.

Monitoring

7. The GOsC will monitor the use of its information processing and storage systems in a manner that is set out in supplementary policies, eg the Email and Internet Policy and Out of Office Remote Policy, to ensure compliance with this policy.

Policy statement

8. It is essential that all GOsC information is adequately protected from events which may jeopardise regulatory obligations. These events include accidents as well as behaviour deliberately designed to cause difficulties. The purpose of this policy is to preserve:

    a. confidentiality: data access is confined to those with specified authority to view the data;
    b. integrity: safeguarding the accuracy and completeness of information and processing methods;
    c. availability: information is delivered to the right person at the right time.

9. The GOsC will develop, implement and maintain policies, supporting procedures and guidance, to achieve appropriate levels of information security. These will cover the range of elements that need to be addressed in the management of information security, in particular the following policy requirements:

Authorised Use

10. The GOsC's information processing and storage systems, will be protected against unauthorised access, and must only be used for authorised purposes. Only persons authorised by the GOsC are entitled to use the GOsC's information processing and storage systems.

Acceptable Use

11. Information is an asset of the GOsC and all employees and other users have a responsibility for protecting that asset from unauthorised access, modification, destruction or disclosure. A serious view will be taken of unauthorised disclosure of information to unauthorised personnel, and disciplinary action may be taken.

Protection of Software

12. The Head of MIS and Registration is responsible for the purchasing, installing, upgrading, removing, and registering of all software for the GOsC. All other users are prohibited from performing any of the above tasks on the GOsC systems without the prior approval of the Head of MIS and Registration or the Chief Executive. All users should be aware it is an offence to copy software or licensed products without the permission of the owner of the copyright.

Retention and Disposal of Information

13. All GOsC employees, including temporary staff, as well as contractors, non-executive members (Council, committee members etc), GOsC associates and other authorised users of GOsC information storage and processing systems, have a responsibility to consider security when creating, using and disposing of information owned by the GOsC. Procedures for the disposal of information (which may involve destruction of the information or the transfer to archival storage) at the end of the retention period, will be documented. Each department will establish procedures appropriate to the information it holds and processes, and ensure that all staff and other users are aware of those procedures.

    Evidential weight and legal admissibility of information stored electronically will be considered when developing procedures for retention and disposal.

Virus Control

14. Virus protection programs will be installed and executed regularly on each file server and the GOsC computer system. It is a disciplinary matter to knowingly introduce a virus or take deliberate action to circumvent precautions taken to prevent the introduction of a virus.

Business Continuity

15. The GOsC's Audit Committee will recommend to the Council approval of a Business Continuity Plan (BCP) aimed at counteracting interruptions to normal GOSC activity, and protecting critical processes from the effects of failures or damage to, vital services or facilities. The (BCP) will include a Disaster Recovery Policy and will be kept under review by the executive and the Audit Committee.

Information Security Incident Reporting

16. All GOsC employees, including temporary staff, as well as contractors, non-executive members (Council, committee members), GOsC associates and other authorised users of GOsC information storage and processing systems, should report immediately to the Head of MIS and Registration, either by email to: acurrie@osteopathy.org.uk, or by telephone: 020 7357 6655 extn 233:

    a. any observed or suspected security incidents where a breach of the GOsC's information security policies has or may have occurred; or
    b. any information security weaknesses in, or threats to, information processing or storage systems.

Legal and Contractual Requirements

17. The GOsC will use its best endeavours to meet its legal and contractual obligations with regard to holding and processing information. This includes relevant European Community and UK legislation, and particularly, the following Acts:

    Computer Misuse Act (1990)

    Copyright Designs and Patents Act (1988)

    Data Protection Act (1998)

    Freedom of Information Act (2000)

Human Rights Act (1998)

Regulation of Investigatory Powers Act (2000)

and the guidance contained in the Information Commissioner's Codes of Practice.

Responsibilities

18. The GOsC's Chief Executive and Registrar has ultimate responsibility for ensuring that the GOsC's information and associated information processing and storage systems are adequately protected.

19. The Council is responsible for approving this policy.

20. The owner of this policy, the Head of MIS and Registration, is responsible for leading on information security issues. This includes providing advice and guidance on information security best practice to managers, who are responsible for maintaining policies and procedures which support this policy.

21. The Head of MIS and Registration is responsible for ensuring that the GOsC's information and associated information processing and storage systems are used in accordance with this policy, and supporting policies and procedures.

22. All authorised users, which includes Council and committee members and GOsC associates, of GOsC information processing and storage systems, are responsible for protecting the GOsC's information assets, and associated information processing and storage systems, and will protect likewise the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations.

23. GOsC employees who have responsibility for GOsC information assets or associated information processing and storage systems, must ensure that appropriate security arrangements are established and maintained for them.

Policy Awareness and Disciplinary Procedures

24. This policy will be made available to all GOsC employees, including temporary staff, as well as contractors, non-executive (Council and committee) members, GOsC associates and other authorised users of GOsC information storage and processing systems. Users will be asked to confirm that they have read and understood this policy before being given access to GOsC information processing and storage systems.

25. Failure to comply with this policy may result in disciplinary action which, based on the nature and severity of the violation, may include the termination of a contract of employment and/or legal action.

Information Security Education and Training

26. The GOsC recognises the need for all GOsC employees, including temporary staff, as well as contractors, non-executive (Council and committee) members, GOsC associates and other authorised users of GOsC information storage and processing systems, to be aware of information security threats and concerns, and to be equipped to support the GOsC in the effective implementation of this policy, in the course of their work for the GOsC. Appropriate training and information on security matters will be provided for all users. The owner of this policy will undertake a proactive campaign to raise information security awareness for all users.

Maintenance

27. This policy will be maintained by the Head of MIS and Registration, and reviewed by way of written report to the Senior Management Team, at least annually and at other times as necessary. Revisions will be subject to appropriate consultation and SMT approval.

28. The owner of this policy will report to the SMT on any issues arising from, and bringing forward appropriate recommendations for changes to, this policy. Reports will also be made to each meeting of the GOsC's Audit Committee along with any recommendations for amendments to the policy.

29. Owners of GOsC information or associated information processing and storage systems, are required to carry out assessments of information security risks, taking account of controls in place, and establish and maintain effective risk management plans. They must also take into account, changes in business requirements, changes in technology, and any changes in the relevant legislation, and revise their security arrangements accordingly.