

SERVICE BRIEFING: POLICIES, PROCEDURES & STANDARDS

Objectives

A comprehensive set of documented policies, procedures and standards is central to the implementation of an effective information security regime. These documents define the way in which information security is managed across the organisation, and set the security agenda. They are also the necessary starting point if an organisation needs to comply with a particular set of information security standards (ISO 17799, ISO 27001, CoBIT, SOX etc.) for regulatory reasons. The objectives in this type of project are therefore usually as follows:

- i. to create a comprehensive set of information security policies, procedures and standards that are appropriate and realistic for the client
- ii. to ensure that they are consistent with any specific standard set mandated by the client's legal or regulatory environment
- iii. to ensure that they are rolled out and presented in such a way as to maximise the likelihood of internal compliance

Scope

The scope of the policies, procedures and standards will cover all "controls" (both technical and procedural) necessary to ensure that an appropriate level of security is in place to protect the availability of critical IT systems and data, and to protect the confidentiality and integrity of data across the organisation. Where the client's requirement is to achieve compliance with a mandated information security standard then this will determine the precise scope of the policy set. Where there is no specific mandated standard, the policies, procedures and standards will be based on the operational needs of the client taking into account their risk profile, resources, operational imperatives and what will be necessary to demonstrate compliance with applicable legal requirements. The policies, procedures and standards will typically cover each of the following areas:

- Roles and responsibilities in managing security
- Third party access to the network
- Remote access
- Information management (encryption, confidentiality etc)
- Security incident management
- "Acceptable Use" Agreement for all staff
- Physical access controls
- Protection against malware
- Secure configuration of different types of computing equipment
- Back up procedures
- Wireless computing
- User access management
- Authentication controls
- Change management
- Disaster recovery
- IT asset management
- Maintenance and protection of IT assets
- Software development lifecycle


Methodology

The methodology will typically comprise the following steps:

- i. review of existing documentation
- ii. structured interviews with key personnel responsible for the implementation of security controls
- iii. policy workshop to discuss identified issues
- iv. creation of first draft, and subsequent review process
- v. creation of final draft
- vi. presentations to all personnel to ensure "buy in" and understanding

Deliverable

The deliverable will be a comprehensive set of policies, procedures and standards tailor made to meet your organisation's operational and compliance requirements.



A comprehensive set of policies, procedures and standards is a fundamental prerequisite for any information security regime.

Contact Safecomms

Tel: +44 1223 576 044
Fax: +44 870 836 2157

info@safecomms.co.uk

16 Millers Yard,
Mill Lane
Cambridge, CB2 1RQ
United Kingdom

