

IT SECURITY POLICY DOCUMENTATION

The SELEX Communications Consultancy Group has extensive experience of developing IT Security Policy Documentation (SPD) for the public and private sectors.

Our consultants have produced security documents for major Defence projects, multi-nationals and small enterprises. In each case, our consultants focus on the needs of the business, producing documents that are tailored to the organisation.

OVERVIEW

Security Policy Documentation (SPD) is the foundation for effective, consistent security throughout the enterprise, whether large or small. A clear, concise policy statement lays down the security framework, and communicates to all members of staff their duties and responsibilities. SPD also provides the basis for managing risk, and applying security measures where they will be most effective, providing the basis for cost-effective, secure solutions to business needs.

Every organisation should have a security policy that identifies the critical assets of the organisation and how they will be protected. But that policy, and the processes and procedures to implement the policy, needs to be tailored to the business.



PUBLIC SECTOR

The Manual of Protective Security (MPS) is the manual with which individual policies must comply. Some Departments, such as the Ministry of Defence, have their own corporate security policy document based on the Manual of Protective Security, but including additional detail depending on their function.

Our CLAS consultants have expert understanding of the MPS, the Defence Manual of Protective Security and other departmental policy manuals; having produced Accreditation Document Sets based on the corporate standards for many different systems.

Working in close consultation with project staff, our consultants can advise on all aspects of information assurance, and produce SPD to support business decisions as the project develops. From initial risk assessment, based on the value of information assets and business requirements, through test and acceptance criteria, to operational security processes and procedures, we provide the documentary evidence to support business and risk management decisions.

All of our consultants are cleared to at least Security Check (SC) level.

PRIVATE SECTOR

SELEX Communications can help private companies that do not have security policies develop their own, tailored to their business and working practices. Using experience gained in public and private sectors, our consultants can produce security policy documents that make sense for your business.

We produce the full range of documents needed in modern business, ranging from Acceptable Use policies for all members of staff, to User Guides and procedures for remote workers, as well as technical security instructions for IT managers and system support staff.

We can also produce Incident Response Plans and Business Continuity Plans, based on the needs of the organisation and the resources available.

In all cases, our procedures are based on the needs of the business, and help to make security a business enabler, exploiting the gains in efficiency and productivity that modern information systems promise. Expensive technical solutions lose their effectiveness if staff do not apply the most basic security rules. Clear, simple security policies and procedures help communicate the essential requirements to users, and assist in building an awareness of the need for security.

Our experienced security consultants take care to ensure they understand the business and the existing culture, producing policies and procedures that are workable and effective.

ABOUT SELEX COMMUNICATIONS

SELEX Communications is a world leader in the development and supply of information security products and services to military, government and commercial organisations.

We have earned a reputation for excellence in this specialised field, offering secure solutions for fixed and mobile communications networks.

Through continued development, the consultancy group now contains accredited experts in the fields of penetration testing, network design, architecture and security, policy writing, contingency planning, forensics, risk assessment / gap analysis and ISO/IEC 17799 (BS 7799) auditing.