



**The right steps to an  
effective security policy**



**Policy and processes**





## **Security policy:** guidance at every level.

*Having a security policy is one thing. Making it actually work is quite another. One of the single most important factors in any organisation's efforts should be its security policy: this should define an organisation's stance to information security and what is or isn't deemed acceptable working practice. In essence, a "one-stop shop" for any employee requiring security guidance.*

### **The first steps**

In too many organisations the IT security policy is left out-dated, forgotten and not within easy reach of general staff, and is all too often seen as a list of "do not's", rather than something that can actually enable business.

Sec-Tec's services for the creation, review and updating of an IT policy can shine a refreshing new light on any security documentation, whether from the initial concept or simply bringing a fresh perspective on the whole process. We understand that, although it is a vital tool in any organisation's security arsenal, there is no wrong or right way to create a security policy; instead, there are degrees of effectiveness and a security policy should be considered by all in order to enhance business, not to act as a barrier.

A good security policy is light, easy to read, but also detailed where necessary. It will often include as part of its content vital information such as an acceptable usage policy for staff and a code of connections for third parties connecting to the corporate network for support and system management purposes.

### **Higher standards**

Another benefit to implementing a sound IT security policy is the fact that it is often the first step towards obtaining an ISMS (Information Security Management System) compliant to BS7799: a standard in which more and more organisations are now striving for certification.

### **Review**

But, like most things in the world of information security, a security policy needs to be regularly reviewed and updated.

To quote just one example: malicious mobile code in the 1980s caught many organisations unawares, creating all sorts of problems.

Sec-Tec can help an organisation review its current information security policy in a critical but constructive light. We can assist with updates, or we can teach an organisation how to become self-sufficient in this vitally important task.



## FAQs

### **Do we need a security policy?**

Every organisation requires a security policy. It is, beyond doubt, the single most important factor within information security. It acts as a one-stop information source for the entire organisation, often detailing a far wider range of measures than technology itself.

### **What does a security policy help us achieve?**

A security policy helps in a myriad of instances where technology cannot cope. For instance, dealing with paper documents, physical security, and even disaster recovery, falls within the remit of a security policy.

### **Can a security policy be created in-house?**

An in-house created security policy is perfectly acceptable. In fact, even when an external organisation is tasked with the creation of a security policy, only the clients themselves can determine what is and is not an acceptable business risk. For this reason, Sec-Tec works very closely with all its customers at every stage of policy creation or, if required, can simply cast an experienced eye over the current policy.

### **Does a security policy make an organisation BS7799 compliant?**

No, but the security policy forms an essential part of the overall ISMS (Information Security Management System) which is at the heart of BS7799 compliance. An aligned security policy is therefore often seen as one of the first steps towards compliance or alignment with the Standard.

## Considerations

The following points represent a small selection of the areas of IT security that should be considered when creating or reviewing a security policy:

- **Network access** –
  - password strength
  - users' choice of passwords
  - frequency of password renewal
  - procedure when a password is compromised
  - ex-employees' login removal
- **Data security** –
  - sensitive data access
  - encryption
  - e-mail security procedures
  - portable PCs
  - external access to the LAN
- **Perimeter defence** –
  - firewall: ITSEC- or Common Criteria-certified
  - configuration auditing
  - change control procedure
  - bypassing of the firewall by internal users with modems
- **Internet usage control** –
  - activity and monitoring
- **Virus control** –
  - deployment
  - layers of AV protection
  - frequency of AV updating
- **Legal issues** –
  - Data Protection Act
  - new Human Rights Act amendments
  - RIP Bill
- **Illegal software** –
  - software licence infringement
  - regular audits reconciled against licences
- **Off-site transport of data** –
  - use of laptops by staff and third parties
  - data transport via CD, paper, etc
- **Backups and storage** –
  - disaster recovery

Once created, all security policies will also need constant updating and amending.



[www.sec-tec.co.uk](http://www.sec-tec.co.uk)



**Tel:** +44 (0) 20 8317 7962  
**Fax:** +44 (0) 20 8317 8051  
**Email:** [info@sec-tec.co.uk](mailto:info@sec-tec.co.uk)  
**Web:** [www.sec-tec.co.uk](http://www.sec-tec.co.uk)

