

INFORMATION SECURITY: HOW TO WRITE AN INFORMATION SECURITY POLICY

[Introduction](#)

[Why have a policy?](#)

[What is a policy?](#)

[Document structure](#)

[Sources of policy](#)

[Authorisation, implementation and operation of policies](#)

[Summary](#)

[Further help and advice](#)

Introduction

This section is intended to help you produce an information security policy. Some of the information contained here is of a particularly detailed and complex nature and may not, therefore, be relevant for all companies.

We have, however, tried to ensure that there is advice for all organisations, irrespective of size or experience.

Producing an information security policy should not be seen as a difficult task. What is important is that it should give clear policy direction and management support for the implementation and maintenance of information security. To be effective the policy should be relevant, accessible and understandable to all intended users throughout the organisation.

A policy needs management commitment, supporting procedures, an appropriate technical framework within which it can be implemented, a suitable degree of authority, a means by which compliance can be checked and a legally agreed response in the event of it being violated.

Sound policies are the basis for good information security. Their role is to provide focus and direction and act as the element that binds all aspects of information security management.

The characteristics of any policy depend on many factors. These can be collectively described as the culture of the organisation. Some organisations have a strong 'command and control' culture. This can result in policies that contain strong, imperative statements (for example, 'You will log off at the end of each working day.'). Other organisations may use subtler phrases, designed to persuade those who are subject to the policy.

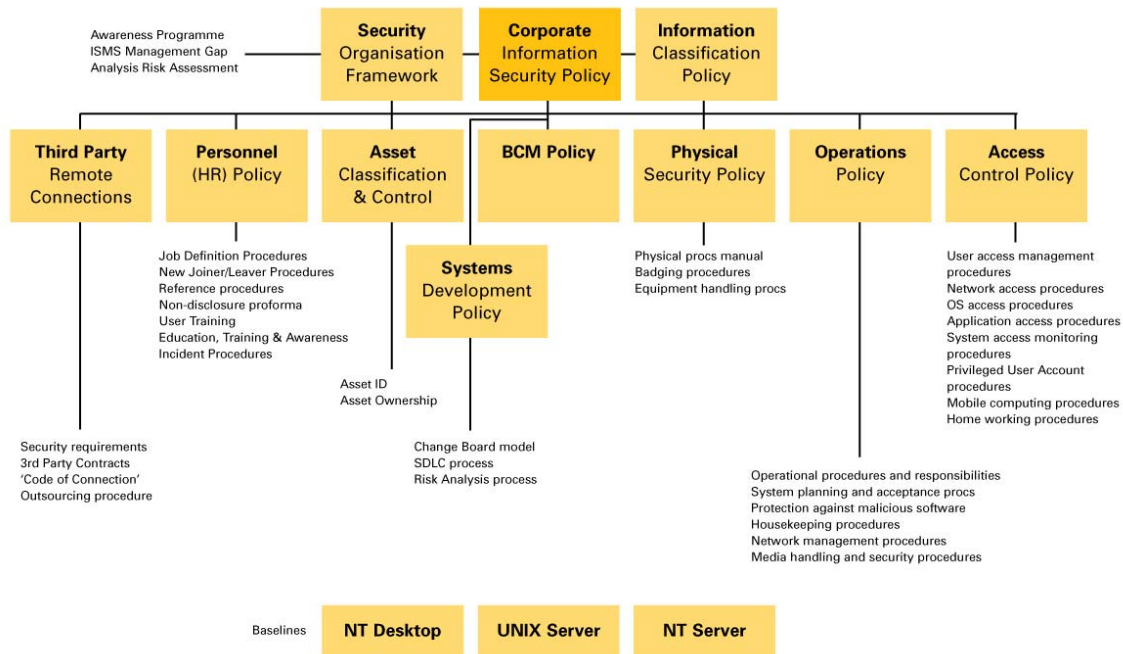
Whichever culture or management style your organisation adopts, the purpose of an information security policy is to help to manage risk and reduce it to an acceptable level.

Why have a policy?

As companies grow, previous methods of communication can become less effective. For example, informal understandings and chats in the corridor can prove insufficient. Legal and regulatory pressures increase as companies expand. Providing the entire company with clear, concise, internal governance can bring real benefits in terms of efficiency as well as a means of reducing information risk. A clear information security policy can:

- reduce ambiguity
- provide clear management direction and commitment
- establish agreed roles and responsibilities

Consideration of the above points can provide a means of dealing with the inevitable difficulties that emerge when managing information. Such difficulties may include balancing the need to share information with the need to restrict its access. Policy is an expression of intent. It needs to be supported by subordinate policies and pragmatic procedures. An outline map of a full document set is shown below:



What is a policy?

There are many different terms in use to describe an information security policy. In the USA, for example, it is common to use the term 'policy' for documents that are often described in the UK as 'standards'. This can lead to misunderstanding. The model in this document uses the following terms:

- corporate information security policy
- specific policies
- standards
- procedures

Corporate information security policy

A corporate policy sets out an organisation's intentions and principles regarding information security. It should be timeless in that it should alter little from year to year. Corporate policy must:

- be clear and unambiguous
- include statements covering:
 - scope
 - legal and regulatory obligations
 - roles and responsibilities
 - strategic approach and principles
 - approach to risk management
 - action in the event of a policy breach.

The policy should be endorsed at the highest level – for example, by the MD or Chief Executive.

Specific policies

These change more rapidly than corporate policies. As they are more detailed they need to be reviewed more regularly. Examples of specific policies include:

- information classification
- access control
- operations
- incident management
- physical security
- human resources
- third-party access
- business continuity management

Standards

Security standards provide guidance towards achieving specific security policies, often related to particular technologies or products. They are used as a benchmark for audit purposes and are derived from:

- industry best practice
- experience
- business drivers
- internal testing

They must be reviewed regularly to ensure that new releases and vulnerabilities are addressed. Examples of standards include:

- UNIX server builds
- firewall configurations
- connectivity protocols

Procedures

Procedures should be:

- clear
- unambiguous
- up-to-date
- tested
- documented

Examples of procedures include:

- incident reporting
- incident management
- user ID addition/removal
- server backup

Document structure

You may find that you need to adhere to an already established format for publishing internal policies. It is not always possible to follow the suggested headings below, but you should attempt to do so.

Note that this format is suggested for specific policies rather than the corporate information security policy that has been outlined previously.

Suggested headings for internal policies

These are listed below and subsequently summarised in bullet points:

Summary

Version number and change record

1.0 Introduction

1.1 Definitions and scope

1.2 Authority (including any legal or regulatory issues)

2.0 Objectives and basic principles

3.0 Roles and responsibilities

4.0 Policy

4.1 Statement heading 1

4.2 Statement heading 2

4.3 Statement heading 3 etc.

- The **summary** is straightforward, providing a single page (maximum) of information that allows the reader quickly to understand the purpose, authority and scope of the policy.
- The **version number and change record** are important as they ensure that the most up-to-date policy is applied.
- **Definitions** (especially of technical terms) are essential. There are some terms (such as 'integrity') that have a very specific meaning in the context of information security. All such terms should be explained in this section. It's important to remember that you are not trying to provide a true dictionary definition; the definitions should be used in the context of the policy (make sure you use the same definitions across an entire document set).
- The **scope** of the policy should define those people to whom the policy applies, and in what circumstances. There may, for example, be policies that apply solely to full-time employees. Others may apply specifically to senior managers while further policies may only be relevant in certain circumstances, such as night shifts or when staff are traveling abroad.

- Each policy should include details of whatever **authority** supports the policy (such as the Board, the Company MD or the Head of HR).
- Each policy should have a set of **objectives** (if you can't define these, you should consider your reasons for having the policy in the first place). The **basic principles** include statements such as 'We will operate on a "need-to-know" basis' (or conversely, 'on a "need-to-restrict" basis'). This enables you to establish the principles by which you wish to operate. They are related to, but independent of, actual policy statements.
- Roles and responsibilities are related to the scope statement. As an example, the following roles and responsibilities can be agreed and published.

The Board is ultimately responsible for ensuring that information security is properly managed. The Information Security Manager is responsible for:

- the development and upkeep of this policy
- ensuring this policy is supported by appropriate documentation, such as procedural instructions
- ensuring that documentation is relevant and kept up-to-date
- ensuring this policy and subsequent updates are communicated to relevant departments and personnel.

All staff are responsible for adhering to this policy, and for reporting any security breaches or incidents to the Security Manager.

- **Policy statements** should be unambiguous, concise and establish intent. The following statements are provided as an example of what you might expect to see in the management of highly privileged computer user accounts.

Privileged accounts

The setting up of privileged accounts should be kept to the minimum. Formal processes will be applied in cases where it is considered appropriate to issue special privileges to users. These processes will:

- identify the privileges associated with each component of a system (e.g. the operating system, database management system or application)
- identify the categories of user requiring special privileges (e.g. 'system administrator')
- allocate privileges on a restricted basis (e.g. 'need-to-use' or 'event-by-event' basis)
- maintain a record of privileges allocated
- ensure that the authorisation process has been completed before privileged access is allowed.

Users issued with special privileges will have different IDs for privileged and non-privileged accounts. Group user IDs should only be used in special cases.

Sources of policy

Policies are normally based on existing, published standards, such as ISO/IEC 27001, which provides a specification for an information security management system (ISMS).

At the very highest corporate level, there are risk management-related publications (such as the Cadbury and Turnbull reports – see www.ecgi.org and www.icaew.co.uk/internalcontrol) that have had considerable impact. The sections below provide a number of potential sources of policy-related material.

The ISO/IEC 27000 standards

ISO/IEC 27002 is a code of practice for information security management. It is designed to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used. This code of practice started life as the UK standard BS 7799-1 in 1995 and was then released as an international standard in 2000 and revised in 2005 in line with normal ISO procedures. It was renumbered as ISO/IEC 27002 in 2007.

ISO/IEC 27001 (previously BS 7799-2) provides a specification for an information security management system (ISMS). This includes a number of processes for designing, implementing, maintaining and updating an ISMS. ISO/IEC 27001 can be used for ISMS certification according to the European standard EN45012 and the accreditation guidelines standard ISO 27006 (previously EA 7/03). Further developments in information security standards are ongoing and a “family” of such standards now features in the ISO 27000 series.

Further information about the 27000 standards as well as the worldwide register of organisations which have gained accredited certification to ISO 27001 can be found at: <http://www.iso27001certificates.com/>

The UK ISO/IEC 27001 User Group exists to promote awareness of, and share good practice in relation to, ISO/IEC 27001 and information security management systems. Membership (the Group is free to join) benefits include workshops and newsletters. The Group’s [website](#) provides further information.

All these standards and guidelines can be purchased from BSI (www.bsi-global.com) or ISO (www.iso.ch)

BSI IT security baselines

The Bundesamt für Sicherheit in der Informationstechnik (BSI) is a German government agency tasked with producing standards for IT security for the federal government. The agency has an English version of its IT Baseline Protection Manual which is designed to:

- help solve common security problems
- create a baseline of security for IT systems
- simplify the creation of IT security policies

This document provides in-depth guidance (over 1600 pages) and baseline controls. The baselines have a strong technical bias and are aimed at IT security professionals, although they do provide a good source of sound advice. The baselines are regularly updated and are available in many formats (to download, in hard copy or on CD). Most of these are free of charge, but check the web site (www.bsi.de) for further details.

COBIT

The Control Objectives for IT (COBIT) were designed as a control framework that combines widely accepted control objectives and a supporting toolset. COBIT has a range of products, including a management guide, control objectives and related support material. It was produced by ISACA (Information Systems Audit & Control Association – the internal audit professional representative body) and although aimed at audit professionals, it provides a robust framework for the larger organisation. There is no proposed certification process as COBIT depends on ISACA certified auditors (with the appropriate qualification) as the main controlling body. Most of the document set is freely available in English from www.isaca.org

GASSP

The Generally Accepted System Security Principles (GASSP) were originally developed by the Computer Security Institute in order to meet US government needs.

They are based on multiple sources, including OECD guidelines and BS 7799. They are aimed at general management as well as information security specialists, and are freely available in English from:

- www.gocsi.com
- web.mit.edu/ist/topics/security

Information Security Forum (ISF) Standard of Good Practice

The Standard of Good Practice (SOGP) was designed to provide a target against which ISF members can measure their information security management performance.

It consists of a series of control objectives matched to control statements, which are based on what is considered by the ISF to be 'good practice'.

The SOGP was produced as a result of findings from the ISF survey process (full details of which are only available to ISF members). The SOGP is now publicly available and is aimed at information security professionals. It is updated every two years and is available in English from the following web sites:

- www.isfsecuritystandard.com
- www.securityforum.org

Information Technology Infrastructure Library (ITIL)

ITIL is a collection of best practices in IT service management, consisting of a series of books giving guidance on the provision of quality IT services. ITIL is drawn from the public and private sectors internationally, supported by a comprehensive qualification scheme and accredited training organisations. It includes descriptions of best practice in information security management as well as other related disciplines. For further details visit www.itil.co.uk

Authorisation, implementation and operation of policies

Authority

You will need to ensure that your policy and supporting documents are appropriately authorised. In some organisations, the MD's signature may suffice. In many other companies it is best to seek authority from a broad range of senior executives, perhaps in the following departments:

- finance
- operational heads
- personnel/HR
- legal

Implementation

It would be difficult to implement an entire policy document set across an organisation at any one given time. A phased approach usually works best, choosing an area with easily defined boundaries and one which supports a range of other services, e.g. the central IT function.

Why the central IT function?

- This is normally a critical internal service provider in which high assurance is essential.
- Much security is delivered through technology.
- IT provision is often already well managed.
- The scope does not have to include all users.
- Subsequent phases can concentrate on core business and IT end-users, as the IT function will then be compliant with policy.

A second target could be the personnel or human resources function. The reasons for choosing this are broadly similar to those for initially choosing the IT function.

Subsequent target areas will benefit from this work, and it will be easier to implement policies as central 'service providers' will be covered by the policy already.

Operation

As part of the broader issue of managing information security comes the need to monitor compliance with (and effectiveness of) your policies. You will find that some policy statements are not adhered to (e.g. people may share passwords). This can be because they would detract from normal work, or are perceived as being excessively costly.

In most cases the key to effective security is to set policy that can be achieved and to ensure compliance. You will also need to have suitable processes for dealing with the inevitable, but few, valid policy exceptions. However, be prepared to modify your statements based on feedback. People will comply more readily if they have been involved in policy development and feel they are stakeholders.

In time, the policy set should become the benchmark for any audit processes used.

Summary

- Writing a policy is easy. Implementation can be more difficult.
- Get 'buy-in' to a policy from senior management. If people are involved in the developmental stage, they are much more likely to comply with policy requirements.
- Obtain the appropriate authority for a policy. Make sure it relates to your corporate culture.
- Policy is only part of a broader set of control-related elements that make up information security.
- Implement a policy gradually.
- Don't reinvent the wheel. Use policy templates such as the one contained in the BERR publication "[Information Security: A Business Manager's Guide](#)", and standards such as ISO/IEC 27001 and 27002.

Please refer to the section on [Legislation, Policy and Standards](#) in our business advice pages (see below) for further information.

Further help and advice

General

BERR Information Security Health Check Tool
<http://www.securityhealthcheck.berr.gov.uk/>

BERR Information Security Home page
www.berr.gov.uk/sectors/infosec

BERR Information Security Business Advice pages
<http://www.berr.gov.uk/sectors/infosec/infosecadvice/page10059.html>

BERR Information Security Publications (available to order or download)
<http://www.berr.gov.uk/sectors/infosec/infosecdownloads/page9935.html>

Published by the Department for Business, Enterprise & Regulatory Reform
www.berr.gov.uk

© Crown Copyright. URN 09/643.