

WHITEPAPER

Information Security Policy

Author: MH
October 2002
V1.1

Table of Contents

1	INTRODUCTION	2
2	POLICIES.....	3
2.1	TYPES OF POLICIES.....	4
2.2	CRITICAL FACTORS	5
2.2.1	Management Support.....	5
2.2.2	Involve relevant Stakeholders	5
2.2.3	Develop policies with the intended audience in mind.....	5
2.2.4	Educate and make people aware of the policies	6
2.2.5	Develop policies that support the business.....	6
2.2.6	Be relevant and enforceable.....	6
2.3	TYPICAL POLICIES	6
2.4	POLICY DEVELOPMENT	2

1 Introduction

Managing Security within an organisation is a challenging task. Without a security policy, supporting guidelines and procedures, the challenge is even greater.

A security policy outlines the requirements with regard to information security within an environment. Combined with standards, guidelines and procedures this allows management to take control of information security. What this means in real terms is that employees know what is expected of them, what is acceptable and what is not. This applies to both users of IT as well as to those who manage it.

Without appropriate policies,

- Staff members may be unaware of their responsibilities and duties regarding IT Security. Consequently, they may deliberately or accidentally compromise corporate information.
- Management may have no recourse against perpetrators.
- Staff has no official guideline for configuring and administering systems with regard to IT Security.
- Systems may be secured inappropriately as the value of the information is not known or has not been adequately determined.
- Management may be unable to demonstrate due care and diligence with regards to information security.
- The company, company directors and management may be held liable.

Generally speaking, organisations operating without a security policy have a tendency to have security controls implemented inconsistently. This often results in loopholes that can be exploited or procedures that fail. Furthermore, detecting and resolving these weaknesses can be difficult and time consuming.

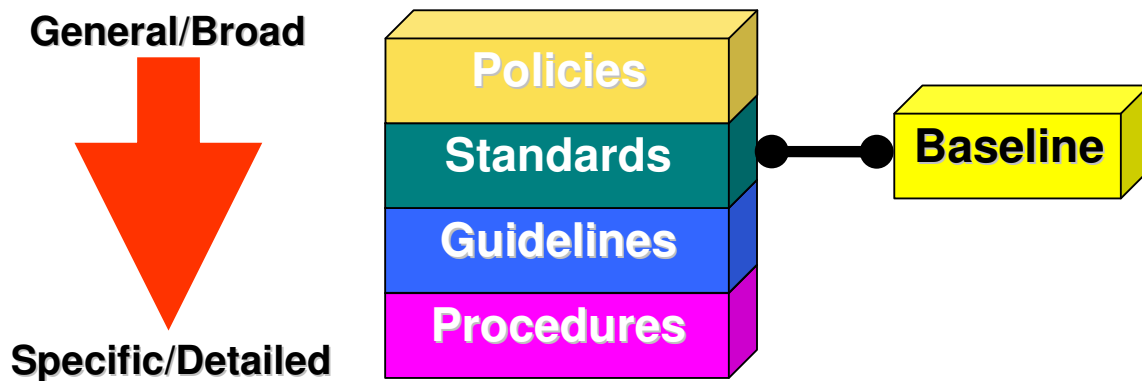
This document provides some general guidelines and ideas when developing Information Security policies.

2 Policies

When discussing policies there is often confusion as to what a policy is and how they relate to standards, guidelines and procedures.

For our purposes we will define them as follows:

- **Policy** – A Policy is a management instruction indicating a course of action, a guiding principle, or an appropriate procedure that is expedient, prudent, or advantageous. They state the role of Security within the organisation. They are high-level statements that provide guidance to staff that must make present and future decisions. They are mandatory and can also be thought of as the equivalent of an organisation-specific law.
- **Standards** – Standards provide specific requirements to be met.
- **Guidelines** - Guidelines unlike policies are optional and recommended.
- **Procedures** - Procedures state how the standards, guidelines and policies are to be implemented.



2.1 Types of Policies

Security policies can be an organisational policy, issue specific, or system specific. Most organisations will have at least one organisational policy, several issue specific policies and some system specific policies. They are further subdivided into three categories Regulatory, Advisory and Informative.

- **Organisational Policy** – organisational policies determine the general direction and outline the importance of information security and how it is to be managed within the organisation, these types of policies assign goals, responsibilities, address laws and regulations. They address all aspects of security.
- **Issue Specific** – Issues specific policies are usually created when there is a need to go into further detail for a specific issue. For example, Internet and Email policies, remote access,
- **System Specific** – this type of policy addresses issues at the system level, for example what software can and cannot be used. Which standards and guidelines must be followed for specific systems.

Within the above three groupings policies are either:

- **Regulatory** – Regulatory policies are those that have been created to address what must be implemented in order to comply with regulations or other legal requirements. For example the Privacy Act.
- **Advisory** – The policies are not necessarily mandated to be followed, however they are strongly suggested and within the organisation they are generally treated as Law with appropriate penalties for non compliance. Most company policies will fall into this category.
- **Informative** – These types of policies inform the reader, they do not imply or require anything.

2.2 Critical Factors

When you are developing and implementing policies there are certain factors that will be critical to the success of the process. The critical factors will determine whether the policy will be appropriate, accepted and is enforceable.

To successfully develop and implement a policy you must:

- Have Senior Management support
- Involve all relevant stakeholders in the development process
- Develop policies with the intended audience in mind
- Educate and make people aware of the policies
- Develop policies that support the business
- Be relevant and enforceable

2.2.1 Management Support

Under various acts such as the Corporations Act, management has ultimate responsibility, this includes responsibility for security.

Companies can be held liable for offences committed using their equipment, especially if it can be shown that due care and/or due diligence is absent.

It is therefore essential that they support and sign off on policy. Without the signoff the process will become difficult and the resulting policy usually will not be accepted by the employees. "If they don't support it, why should I follow it?"

2.2.2 Involve relevant Stakeholders

The best policies have involvement from many different stakeholders. By including different stakeholders you start the process of promoting the policy as well as receive a more accurate picture of the environment and identify more accurately what needs to be included in the policies.

2.2.3 Develop policies with the intended audience in mind

Policies should be developed with the appropriate audience in mind. A policy aimed at IT staff can contain more technical terms than a document aimed at non-IT staff. Audiences differ as does the message that needs to be put across. Policies may need to be broken up to address the appropriate audience

2.2.4 Educate and make people aware of the policies

Education and awareness is the key to policies. A policy of which the employees are not aware is not enforceable. There are many different mechanisms that can be used to disseminate the policies to their audiences. The method that will work best is often determined by the culture of the organisation and the nature of the audience.

When introducing a security policy it is important to have support from both management and the people directly affected by the policy. The way the policy is introduced can have an impact on how it will be accepted.

2.2.5 Develop policies that support the business

For policies to be accepted they must also support the business. Policy statement such as "no outside access to company x owned systems" for example would be inappropriate for someone like Amazon.com. Like any security control polices should support the business goals.

2.2.6 Be relevant and enforceable

Policies should be relevant and applicable to an organisation, "the glass slipper does not fit everyone". The policy statement should also be enforceable. For example "no personal use of email and Internet connectivity is permitted". This statement will be violated within minutes of it being published, in fact as soon as some sends an email along the lines "I'll be working late, don't wait up". If the policy is not enforced at this stage it will not stand up when it is needed. A statement such as "Personal use of the Internet is acceptable where it does not interfere with normal business activities, does not involve solicitation, is not related to for profit activities and must not potentially embarrass the company", would be more appropriate and is enforceable.

2.3 Typical Policies

Following are some of the more commonly found policies within organisations.

- General Security
- Internet access & Email policy
- Confidentiality Agreements
- Remote Access
- Internet Infrastructure Management
- Third Party Access
- Teleworking
- Anti virus
- Data Classification

2.4 Policy Development

After the risks have been identified, a policy can be created to help manage those risks. This is usually easiest to achieve using a "Top Down" approach. Begin with a high level Management statement of objectives. From this policies that are more detailed can be developed concerning mechanisms and standards, which in turn form the basis of specific guidelines and daily procedures. The whole process does not need to be executed in one go, in fact the best policies "evolve" into an environment in an interactive manner, over time.

The need for separate policies is often decided by the topic and the audience of the policy. For example an Internet and email policy applies to all staff, as usually all will be using both the Internet and email, however a firewall infrastructure policy applies only to those staff directly responsible for managing the firewall infrastructure. This separation of topic and audience provides a more focused policy and increases its usability.

Many security policies try to cover all aspects of security in the same document, this usually means the message is lost and the policy becomes unwieldy. The security policy describes the corporate strategy and direction, individual policies focus on particular areas.

Guidelines and procedures help enforce the security policy by giving staff direction on how to implement the security measures, providing a consistent approach to, building servers, responding to security breaches, implementing firewalls, etc. The procedures and guidelines translate the generic language of the policies to the technical implementation of the policy on the specific systems.