

# THE PEN IS MIGHTIER THEN THE SWORD

## PRACTICAL POLICIES FOR INFORMATION SECURITY

(a 4 part series published on Security Focus in April 2001 by Charl van der Walt @ SensePost)

### TABLE OF CONTENTS

<b>1.</b>	<b>Introduction</b>	<b>3</b>
<b>2.</b>	<b>Definitions</b>	<b>3</b>
<b>3.</b>	<b>In praise of policies</b>	<b>4</b>
<b>4.</b>	<b>Policy Power – making policies work for you</b>	<b>5</b>
4.1	Defining the objectives	5
4.2	Setting the stage	6
4.2.1	Management support	6
4.2.2	Organizational structure	6
4.2.3	Finance	8
4.2.4	A culture for security	8
4.2.5	Acceptance	9
4.3	Using a classification system	9
4.3.1	Formal Classification Systems	9
4.3.2	Your own classification system	10
4.3.3	Ownership	10
4.3.4	Classification	10
4.3.5	Clearance	11
4.3.6	Security Levels	11
4.3.7	An example Access Matrix	11
4.3.8	Rules for technology	12
4.3.9	Default Classifications	12
<b>5.</b>	<b>Structuring your policy</b>	<b>13</b>
5.1	Security Framework document	15
5.2	The Security Officer	15
5.3	The Document Manager	15
5.4	Position Papers	15
5.5	Policy Owner	16
5.6	Security Data Sheets	16
5.7	Technical Guides	16
5.8	System Owner	16
<b>6.</b>	<b>Policy Content</b>	<b>16</b>
6.1	Some things each position paper should say	17
6.2	Policies for free	17
<b>7.</b>	<b>Assessing Policies</b>	<b>17</b>
<b>8.</b>	<b>Global Best Practice</b>	<b>18</b>
8.1	Recognition	19
8.2	Focus	19

8.3	Local presence	19
8.4	Cost	19
8.5	Endurance	19
8.6	Objectivity	19
8.7	Conclusion	19
<b>9.</b>	<b>Examples</b>	<b>20</b>
9.1	An IP network security policy	20
9.1.1	Issue Statement	20
9.1.2	Applicability	20
9.1.3	Statement of Foobar's Position	21
9.1.4	Classifications	24
9.1.5	Roles and Responsibilities	26
9.1.6	Compliance	27
9.1.7	Points of Contact and Supplementary Information	27
<b>10.</b>	<b>Conclusion</b>	<b>27</b>
<b>11.</b>	<b>References</b>	<b>28</b>

## 1. Introduction

This is an article about how information security policies can be used as an active part of your organization's efforts to protect its valuable information assets.

In a world that essentially technology driven; where the latest IIS exploit is countered with a mad rush to install the relevant patch and where the number of different operating systems in your network exceeds the number of hairs on your head that haven't turned gray, policies give us an opportunity to change the pace, slow things down and play the game on our own terms.

Many people see policies as an afterthought; a tasty dressing to be added to a veritable technology-salad of firewalls, virus scanners and VPNs, all lightly sprinkled with just a touch of IDS. This is wrong. In this article I'll attempt to explain why policies should be the basis of your Information Security strategy – the dough in your bread – and how policies can be an effective, practical part of your digital defense systems.

## 2. Definitions

### What is a policy?

The nicest definition for 'policy' that I could find is from the *American Heritage Dictionary of the English language*. It reads:

**“A plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters”**

In practical security terms, I define a policy as a *published document (or set of documents) in which your organization's philosophy, strategy, policies and practices with regard to Confidentiality, Integrity and Availability of information and information systems are laid out.*

Thus, a policy is a set of mechanisms by means of which your information security objectives can be attained. Let's take a moment to briefly examine each of these concepts. First, we have the information security **objectives**:

- **Confidentiality**  
is about ensuring that information is only accessed by the people who are authorized to access it. It's about keeping your valuable information secret.
- **Integrity**  
is about maintaining the value of information. Information only has value if we know that it's correct. A major objective of information security policies is thus to ensure that information is modified or destroyed or subverted in any way.
- **Availability**  
is about ensuring your information and information systems are there when you need them. A major objective of an information security policy must be to ensure that information is always available to support our critical business processes.

These objectives are globally recognized as being characteristic of any secure system.

Next, we have the **mechanisms** through which these objectives can be achieved, namely:

- **Philosophy:**  
This is your organization's approach towards information security, the framework, the guiding principles of your information security strategy. Your security philosophy is a big umbrella under which all other security mechanisms should fall. It will explain to future generations why you did what you did.

- **Strategy:**  
Your strategy is your plan. It's the *project plan* of your philosophy. A measurable plan detailing how you intend to achieve your security objectives within the framework of the philosophy.
- **Policies:**  
Policies are simply rules. They're the *dos* and the *don'ts* of information security, again, within the framework of the philosophy.
- **Practices:**  
Practices simply define the *how* of your policy. They are a practical guide regarding what to do and how to do it.

In the sections that follow I'll be examining each of these mechanisms more closely.

### 3. In praise of policies

#### What do policies actually buy you?

In the previous section we covered briefly what a policy is and, more specifically, what an information security policy is. From this brief description it should already be clear that, when it comes to policies, I mean business. And in IT this usually translates to a sizeable investment in time, money and human resources. Don't kid yourself; effective policies are no quick fix. The question on everyone's lips has got to be: "Yes, but what can I do with a policy that I can't do with Snort 1.7 on my favorite Bastion Linux install?" Here are some of the things policies will do for you that you'll struggle to achieve with technology:

#### 1. The boss can do it

Most technological controls are the responsibility of the IS manager, the network administrator or some poor sod who didn't get her leave application forms in on time. Policy, on the other hand, is the responsibility of upper management. This thinking is consistent with company law in most countries that says it's the responsibility of the directors of a company to protect its assets on behalf of the shareholders. Policies are like the hydrogen bombs of your security arsenal.

#### 2. They may just keep your face off *America's Dumbest Criminals*

In some industries your company may have legal obligations with respect to the integrity and confidentiality of certain information. In many cases the only way you can prove due diligence in this regard is by referring to your published policies. Because policy reflects the philosophy and strategy of your company's management it is fair proof of the company's intention regarding information security. Interestingly, an audit against a security standard works on exactly this principle of 'intention'.

#### 3. They impress your friends

Because a policy is typically published, and because it represents executive decision, a policy may be just what you need to convince that potential client / merger partner / investor exactly how clever you really are. Increasingly companies are requesting proof of sufficient levels of security from the parties they link to to do business with. Once again, your security policy is exactly the place to start.

OK, so much for the soft and fuzzy stuff. We said policies can play a *practical* role in securing your information assets. Here's how:

#### 4. They form a benchmark for progress measurement

Policy reflects the philosophy and strategy of management with regard to information security. As such it is the perfect standard against which technology and other security mechanisms can be measured. For example, if you want to know whether your brand new "Hack 'em Back" ultra firewall (performance tested by Russian cosmonauts on Mir) was really worth the price of a small Caribbean island, then check whether it's implementing the controls stipulated in the policy. Similarly, to

determine whether your new IT manager is effectively investing her IT security budget, measure her progress against the policy. And here's the best part: If your policies are correctly formulated and carefully integrated into your employment contracts, then the next that guy with the foot fetish from HR hits [www.kickme.com](http://www.kickme.com) you really *can* get him demoted to washing pots in the canteen. An information security policy serves as a measure against which responsible behavior can be tested.

5. **They help ensure consistency:**

The biggest challenge facing security managers today is not how to negotiate a 512 bit RSA public key exchange using Diffie-Hellman and self-signed certificates (*everyone* can do that these days). No, the challenge is ensuring that the sysadmin in the Tahiti branch gets off the beach in time to load the patch for the IIS *Unicode* exploit on the web server and avoid yet another embarrassing defacement on [www.tahiti\\_branch\\_of\\_my\\_respectable\\_company.com](http://www.tahiti_branch_of_my_respectable_company.com). A well-implemented policy helps to ensure consistency in your security systems by giving a directive and clearly assigning responsibility.

6. **They're your own 'Information Security for Dummies':**

A well-designed policy can become an IT administrator's Bible. Sadly, not everyone who will ever attach a computer to your network understands the threat of TCP sequence number guessing attacks against OpenBSD. Fortunately, your IP network security policy will ensure that machines are always installed in a part of the network that offers a level of security appropriate to the role of the machine and the information it hosts.

7. **They're like having a big stick:**

People can be either the strongest or the weakest link in any information security system. Although training, positive enforcement and technology can all play a role in making people a part of the solution and not part of the problem, in the end there's nothing like a big stick for bringing people over to your way of thinking. An integrated policy can be just such a stick in that it serves as a measure of performance according to which responsible people can be measured and potentially disciplined. As labor law in most countries increasingly favors the employee it's becoming more and more difficult to discipline staff for negligent or malicious behavior. Policies enable us to do just that.

8. **They really are like having a big stick:**

The objectives of information security are often at odds with the desires of system users. How many times has a user thanked you for disabling Active X in her browser and blocking access to *Napster*? Often security staff face resentment and opposition from people in more senior positions to themselves. The policy, as a directive from top management, empowers security staff to enforce decisions that may not be popular amongst system users. Armed with a policy your security administrators can do their jobs without having to continuously justify themselves.

## 4. Policy Power – making policies work for you

OK, OK you're sold. You've seen the light and decided to seriously undertake the implementation of information security policies in your own organization. But how? In the sections that follow I'll try to share with you some of the tricks of the security policy trade.

### 4.1 Defining the objectives

#### What are you actually protecting?

Before making decisions regarding your Information Security strategy (long or short term) you need to achieve an understanding of your organization's unique risk profile.

Risk consists of a combination of information resources that have **value** and vulnerabilities that are **exploitable**. The magnitude of the risk is the product of the *value* of the information and the *degree* to which the vulnerability can be exploited.

As long as your organization has information that has value that, information will be subject to risk. The function of any information security control mechanism (technical or procedural) is to restrict that risk to an acceptable level. This is also true for policies. Policies are a risk-control mechanism and must therefore be designed and developed in response to real and specific risks. Thus, a comprehensive risk assessment exercise must be the first phase of the policy development process. The risk assessment should identify the weakest areas of your system and can be used to define specific objectives.

Of course there is also a sheet-bombing approach to policies and generic policy documents are freely available on the Internet and from various commercial resources. Although there are a number of issues that can be dealt with in a generic manner one should be very careful of this approach. A policy that says too much is no better than a policy that says nothing at all. Remember that you must be prepared to enforce every stipulation your policy makes (I'll say more about this later in this paper) so you want to make your policies focused and specific.

I could give you a packaged speech about the four objectives of information security but you need to define your objectives for your own organization, based on the value of your information and the specific risks that information faces.

## 4.2 Setting the stage

### Creating an environment that supports your objectives.

Policies in themselves are ineffective and their potential to impact is directly proportional to the support they receive from the power structures of your organization. Thus there is a flow of authority that stems from upper management and expresses itself in the implementation of the stipulations of the policies. For this flow to happen certain fundamental changes may have to be made to the structures and culture of your organization. The bigger the organization, the more important these changes become.

Here are some things that will need to be in place before information security policies can have an impact:

#### 4.2.1 *Management support*

I've touched on the importance of management buy-in a few times now already but it's worth stressing again. One of the biggest challenges facing security people is to convince management of the importance of their involvement in the process. Once again risk assessment and penetration testing can help with this. Without the buy-in of management at a high level the policy development process is unlikely to succeed.

#### 4.2.2 *Organizational structure*

No matter what the size of the organization, a policy should always have an owner – typically known as the 'security officer' or 'SO'. It is the responsibility of the security officer to oversee the creation and distribution of security policies. In this sense the SO plays the role of intermediary between management and the user base. It's obvious then that the SO should report directly to the organization's highest level of control – the board of directors or even the chief executive. Because the SO ultimately carries corporate responsibility for information security it is often sensible for him or her to be a member of the board. In a small or medium organization the role of SO may not comprise a full portfolio and could simply be an added responsibility. However, no matter how small your organization the SO role should be clearly assigned and the responsibilities precisely described.

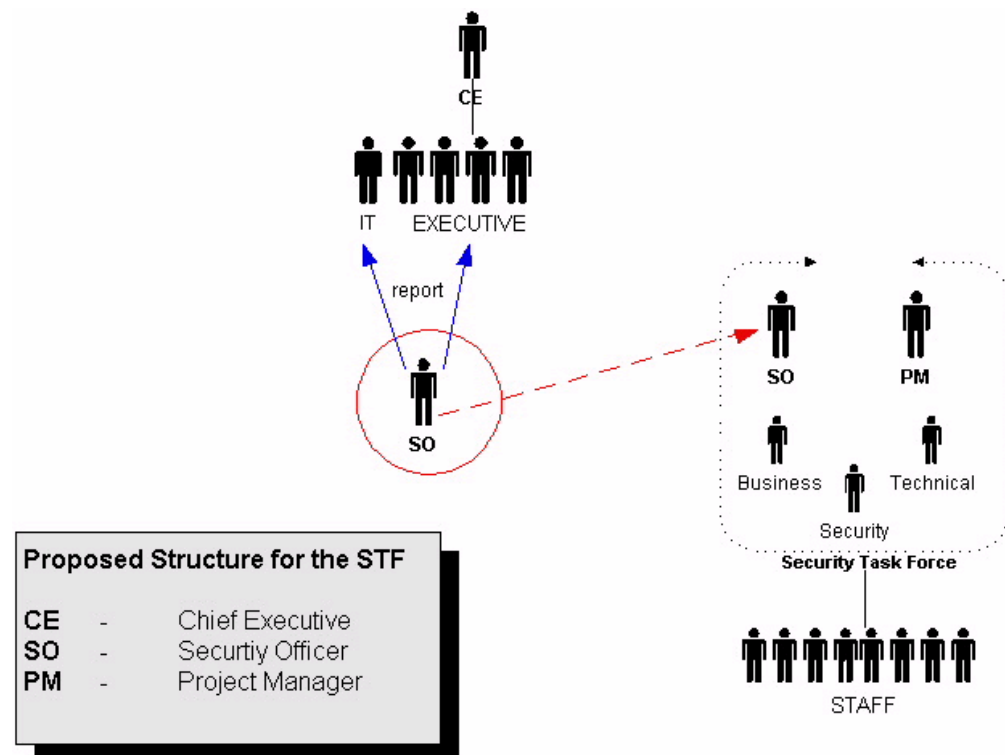
As owner of the policy the SO has a number of responsibilities including, but not limited to the management and distribution of the security policy.

Typically the SO is responsible for aspects of security in the organization, not just issue relating to policy.

It may be that the management structures in your organization have to be adjusted to make provision for the new role.

In large organizations that are still early in the security cycle we often propose the creation of a team or task force (STF) to take responsibility for the security process. Such a team typically consists of the SO, a project manager (PM) and a collection of business, technology and security specialists. The functions of the STF include:

- Defining security strategy
- Creating a mission statement and project planThe investigation of a formal accreditation program (more on this later)
- Defining the corporate security policy
- Defining system specific policies (more on this also)
- A user awareness program
- The appoint of Security AuditorsThe structure of the STF is depicted in the diagram below:



### 4.2.3 Finance

The security process will always require and investment in time, human resources and finance. Without sufficient financial commitment any security effort is bound to fail. The same is true for the policy development process.

In acquiring funds for the implementation of policies we once again see the value of a comprehensive risk assessment exercise. A properly implemented risk assessment should give a good indication of the risk to which your organization's information resources are exposed and the role that policies can play in mitigating that risk. These indicators, combined with a fair understanding of the *value* of your information resources (possibly also gained from the assessment) should provide enough objective data to motivate and scope a financial investment in security.

### 4.2.4 A culture for security

A chain is only as strong as it's weakest link and the weakest link in a security system is very often the end user. I was horrified recently by the potential for abuse created by a new generation of products that allow users to bypass "that pesky" firewall by subscribing to a service that tunnels TCP traffic over HTTP via a Java Applet that runs in any browser. I quote:

*"ABC is a general-purpose tunnel that allows you to pass through that firewall. ABC works by mapping your network requests into web request to our server, so if you can read this page, you can use ABC! ... The uses for ABC are limited only by your imagination. It can pass anything that uses TCP!"*

That means that even if your firewall allows only HTTP requests out, and those only via a proxy that expects user authentication, a clever user can **still** do whatever she wants on the Internet. If your users don't understand the value of your information assets and the risks that these kinds of technologies represent, then you'll be fighting a losing battle. You need to create a culture in your organization that's conducive to the implementation of security policies. I refer to this as "Selling Security" - and it's enough of a subject for an article all of it's own - but here are some strategies that you could consider.

#### 1. ADVERTISE:

Launch an internal advertising campaign explaining the value of your corporate information, the risks that it faces, the role of the policies and the responsibilities of the individual. Consider using a series of slogans like "Your password is you!"

#### 2. FOCUS ON MANAGERS

Management usually sets the tone for the workers underneath them and most passionately enforce the things they personally believe in. Convince the management and half the struggle is won.

#### 3. SPILL THE BEANS

People are generally loyal towards the companies they work for so being honest with staff about security and the impact it has on the organization will usually help to win people over to your cause. One way to do this is to publish the results of security assessments and audits, or to play open cards about hacking and other security incidents.

#### 4. POSITIVE REINFORCEMENT

Because a well-designed policy allows for measurability staff can now be rewarded for good security practice. Perhaps an incentive scheme per department that's based on the results of an annual security audit? Remember, a rule without punishment is just good advice...

## 5. NEGATIVE REINFORCEMENT

I've recently heard of firms that are actually taking disciplinary action against staff for non-compliant or negligent behavior. Once again, policies introduce measurability and make this sort of action possible.

### 4.2.5 Acceptance

All staff should be made to sign a document stating their acceptance of the principles of the security policy. This forces staff to read and understand the policy and gives your organization legal recourse in the case of security breaches.

## 4.3 Using a classification system

**All data are equal, but some are more equal than others.**

In developing your information security policies you'll want to be able to distinguish between various groups of people, computers and information that have differing value and differing requirements in terms of security.

A statement like "Only authorized staff are permitted access to confidential data" isn't worth the disk segment its saved on if you don't clearly define who is "authorized" and what data is considered "confidential". This is no simple task and a large area of work has been done in the security field to answer exactly those two questions (yes, work is occasionally done in the field of security). Most of this work has resulted in one or the other security "classification" system – models by which information resources and people are assigned classification levels which are then used in relatively simple rule statements that describe what people classifications are allowed access to what resource classifications.

### 4.3.1 Formal Classification Systems

Let's briefly explore three such systems, just by way of example:

#### THE MILITARY MODEL<sup>[1]</sup>:

In military circles, it is common for information to be classified into five levels:

- top secret
- secret
- confidential
- restricted
- unclassified

These levels form an ordering with *top secret* at the top, and *unclassified* at the bottom. Users are also assigned a classification, and the following rule is applied:

"To have access to a document, the user must have a classification at the same level as, or higher than, that of the document."

These levels are sometimes known as the *rank* of the information (or user).

Access to military information is also governed by the *need-to-know* principle, which places information in *compartments*. Compartments may extend across security levels, and information and users may belong (have access) to a number of compartments.

The full classification of both information and users is therefore defined by the pair <rank, compartments>.

In the case of users, the <rank, compartments> pair is called the *security clearance* of the user.

## **THE BELL-LAPADULA MODEL<sup>[1]</sup>.**

Bell-LaPadula is essentially a simplified version of the Military model designed to be slightly more user friendly and appropriate to the commercial environment.

Bell LaPadula relies on the fact that there exists a partial ordering on security classifications/clearances.

If  $c(O)$  is the classification of the (data) object and  $c(S)$  is the clearance of the (user) subject then two simple rules (known as “properties”) apply.

1. **The Simple Security Property (ss):**  
A subject (S) may have read access to an object (O) only if  $c(O) \leq c(S)$
2. **The “\*” Property (star):**  
A subject (S) who has read access to an object (O) may have write access to another object (P) only if  $c(O) \leq c(P)$

The first rule is fairly obvious: no-one may receive a piece of information unless their clearance is at least as high as the classification of the information they are accessing

The second states that information obtained from an object may only be passed to another object if the classification of the target object is at least as high as that of the source object. This is to prevent the so-called “write-down” effect in which the classification level of information is gradually diluted as it passed between data objects (e.g. files) of different classifications.

### **4.3.2 Your own classification system**

Now, all of this may seem just a little complex. That’s because it is. Such a formal approach may not be necessary in your organization but there are other approaches and you should develop a classification system and supporting rule set that support your requirements and objectives.

In the next few paragraphs I’ll outline a simple system that can be applied to both *information* and *information technology* and is flexible enough to work in most types of organizations. Later, I will refer to this classification system when I give some example policies.

### **4.3.3 Ownership**

Every piece of corporate data is assigned to an *owner*. By default, the owner is the creator of the data or the person who loaded the data onto your systems. If it is not clear who the owner is, ownership then defaults to the originator or the administrator of the system on which the data resides. The *owner* of a computer system is defined as the head of division requesting the installation of equipment.

### **4.3.4 Classification**

All data has a default classification (refer to the sections that follow) but with sufficient justification, the owner of the data may change the classification. Data may only be changed with sufficient justifiable reason. The user will ultimately be held responsible for data that has been reclassified. If the user is not sure about changing the security level, the Security Manager or divisional manager should be consulted. The person changing the security level will be held responsible for changing the level and must therefore be able to justify the decision.

Computers are classified in a similar way as data. Each computer has an owner - defined as the head of the division requesting the installation of the equipment and it’s the function of the equipment owner to classify all equipment under his or her control. Classification is done in consultation with the owner (or an assigned representative) and the Security Manager but the Security Manager must make the final decision. There may be a pre-defined list of classifications for computers in the network security policy. In

addition to computers themselves, specific services or processes can also be classified. For example, on a UNIX machine used to host web a public web site, the web server may be classified in one way whilst the telnet server has a much higher security level.

The Security Manager must also classify segments of the network and physical locations on the premises to ensure that computers are connected at the correct location on the network.

#### 4.3.5 Clearance

Finally, all users and potential users should be classified. A user's classification is called a *Clearance Level* and is used to determine what data and resources a user may have access to. In general, access is only allowed when the clearance is the same level or higher than the classification of the item being accessed (data, equipment or physical locations).

#### 4.3.6 Security Levels

Let's review the security levels. You must define and describes levels of classification that make sense and are appropriate to your organization. I've already listed the levels typically used in the military model. Another approach may be as follows:

- **Unclassified:** Considered publicly accessible. There are no requirements for access control or confidentiality.
- **Shared:** Resources that are shared within groups or with people outside of your organisation. This can include mail servers that are accessible from the Internet, servers that are accessible from customers and routers that link you to your ISP. Data that is legitimately accessed by outside people or groups can be classified as *shared* and users from outside organizations that have legitimate access to internal resources could also be classified as *shared*.
- **Company Only:** Access to be restricted to your internal employees only.
- **Confidential:** Access to be restricted to a specific list of people. For someone to have access to data or resources classified as 'Confidential' they must be cleared at this level and they must be included in the access list for this resource. The owner of the object (data or computer) is responsible for managing the access lists.

Not only data but also Users are *cleared* according to this system. Every user requiring access to your systems must receive clearance first. This includes employees, contractors, consultants etc.

#### 4.3.7 An example Access Matrix

Once you've finalized a classification system a simple access matrix can then be drawn up:

Access Control Matrix				
USER	OBJECT (Data, Equipment, Physical Location)			
	Unclassified	Shared	Customer Only	Confidential
Unclassified	Allowed	Denied	Denied	Denied
Shared	Allowed	Allowed	Denied	Denied
Company Only	Allowed	Allowed	Allowed	Denied
Confidential	Allowed	Allowed	Allowed	Refer Access List

A matrix such as the one above can form a guide when writing a policy and the example policies given in this document do make use of this system.

#### 4.3.8 Rules for technology

The matrix above deals with **user** access to objects. To describe where equipment is connected to the network, there is a very *simple rule*:

##### The Very Simple Rule:

1. Equipment may never be connected to a network segment with a different security level to that of the equipment.
2. Equipment may never stand in a physical location with a lower security level than that of the equipment.

#### 4.3.9 Default Classifications

It was mentioned previously that objects could have default classifications. The idea behind default classifications is to minimize the workload on users and security staff whilst still ensuring that the proper security controls are always applied.

Here is an example of default classifications:

Default Classifications		
Object Type	Default Classification	To Change Classification
Data	Company Only	User discretion and responsibility
Equipment	Company Only	Request to Security Officer
Network Segment	Company Only	Request to Security Officer
Physical Location	Company Only	Request to Security Officer
User	Unclassified	Request to Security Officer

Of course, all of the above serve as examples only. Obviously, final decisions of classification must lie with the Security Officer and the Security Task Group described earlier in this paper.

## 5. Structuring your policy

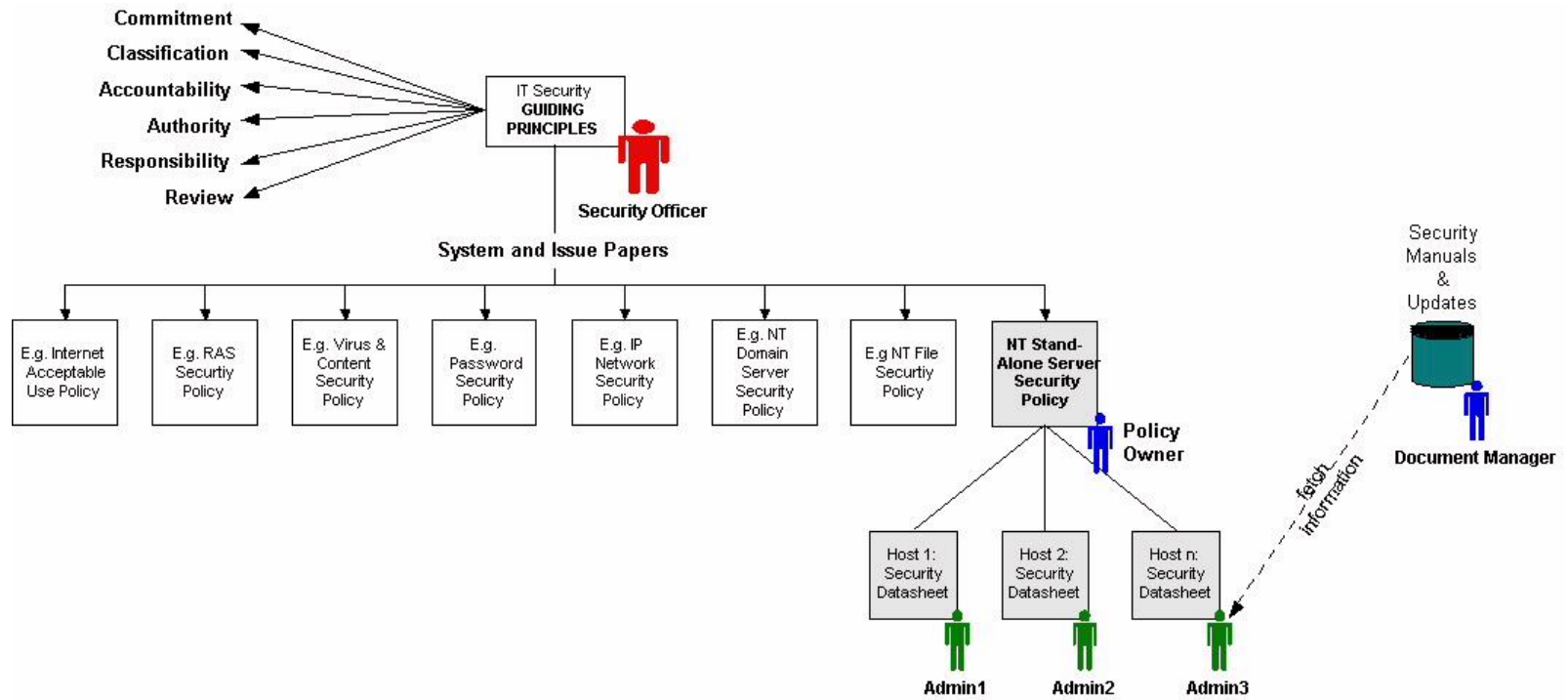
### How do we put it all together?

You can hopefully already see how the use of an effective classification system can help to make your security policies simpler and easier to develop. However, if you're from a large organization and you have a diversity of technologies then the development of policies is still bound to imply a huge volume of work. It is essential that your policies be structured and packaged in such a way that they are as light as possible, without missing any important issues. By "light" I mean the following:

- a) "Light". Not weighing much. Not using too many trees.
- b) Simple and practical.
- c) Easy to manage and maintain.
- d) Easy to access by people seeking specific information.

To meet these requirements I typically recommend that your policy be split into a number of smaller policies and that these be arranged in a hierarchical fashion. The 'smaller' policies I refer to are known as 'Position Papers' and they contain specific policies regarding (yes, you guessed it) specific issues and specific systems. Because each one of these documents is focused it can be kept short and practical, can be written by a specialist and can easily be modified or updated without having any impact on the rest of the policy.

Although each Position paper may be written by somebody different – typically a specialist in that field – we still want all the papers to subscribe to some fundamental principles. These principles (what I call your security 'philosophy') should be laid out in a single document known as the 'Security Framework' paper. This paper, along with the classification system, creates a framework of values and principles upon which each other document should be based. "Security Framework" also forms a kind of *default* policy that can be referred to whenever there is doubt or in cases where there is no policy paper relevant to a particular system. This concept is depicted in the following diagram:



**Information Security Policies: Document and organizational structure**

Let's examine each element of this framework in turn:

## 5.1 Security Framework document

This document defines a minimum set of requirements, applicable to all management, staff and external consultants regarding your organization's information security. The document defines a set of concepts and principles that are designed to ensure the protection of all information assets, irrespective of the nature of those assets or the technologies used to store and transmit them. No decisions regarding the security of information and information technology (IT) should be made without careful consideration of, and due compliance with, the concepts and principles described here.

The Security Framework document should cover at least the following important points:

- a) The **value** of information and your organization's **commitment** to information security.
- b) The **classification system** we discussed in the previous section.
- c) The principle of **accountability** – that users and administrator's will be held accountable for behavior that impacts the security of information
- d) The designation of **authority** to the Security Officer and other security-related roles in the organization.
- e) The principle of individual **responsibility** by all system users for the security of information resources.
- f) The organization's approach to **security reviews** – how often they will take place, who will perform them etc.

## 5.2 The Security Officer

The function and responsibilities of the Security Officer have already been covered in some detail. The SO assumes ultimate responsibility for security in the organization. It is her job guide, advise and review. The "Security Framework" document thus usually falls under the SO, as does the management and distribution of the various position papers.

In a large organization the SO may have a dedicated *Document Manager* on her team – someone whose specific responsibility it is to ensure that all the policy documents are kept current, that changes are properly controlled and that users have free and easy access.

## 5.3 The Document Manager

The document manager is a member of the *Security Task Force* I referred to *earlier* and is responsible for the archival and maintenance of all IT Security Policy documents. A current copy of each policy document and all supporting documentation can be always obtained from the Document Manager.

In a smaller organization this may simply be another responsibility of the Security Officer.

## 5.4 Position Papers

Position papers are written to address the security of some specific technology, or to address the question of security with regard to a particular situation. For example, one might have a position paper covering the secure configuration of Windows 2000 member servers that are connected to the Internet as well one describing the process to be followed in the event that a staff member is found in breach of security policies. Exactly what papers are needed is varies from organization to organization, but I make some comments on this question a little later in this piece.

The papers relate the concepts of the *Security Framework* document to specific problems or technologies in a way that is short, simple, practical and easy to understand. Because these papers are so focused they can be kept short and to the point. They are easily modified and can be written by someone who is an expert in that particular field. Each paper has an owner.

## 5.5 Policy Owner

The Policy Owner is the person responsible for the maintenance and integrity of a given policy document. No changes may be made to a document without the express permission of the Policy Owner. The name of the Policy Owner must be clearly displayed on the document and the document should always be dated and signed by the owner.

## 5.6 Security Data Sheets

I typically recommend that each IT system have a *Security Datasheet*. The datasheet document lists specific settings and parameters that impact the security of that host. Whereas this *Security Framework* and the various *Position Papers* are relatively generic, the datasheet introduces the detail component for each system. Each system or host should have a datasheet that is managed by the *system owner* and is subject to the principles of this document and the *System Paper*.

It is the responsibility of information and technology owners and users to obtain the relevant papers from the SO or the STF and ensure that the standards defined therein are correctly implemented on the systems they control.

## 5.7 Technical Guides

Another set of useful documents (although not actually policies) is technical documentation. We often encourage large organizations to have experts create simple technical guidebook for the configuration and administration of specific systems that can be stored along with the policies and referred to by the position papers. For example, instead of using a position paper to describe exactly how your Solaris-based Apache web servers should be configured, why not write or even purchase a guide that covers exactly that. Again, this contributes to the modular nature of your security policies and makes them both easier to use and easier to manage.

## 5.8 System Owner

We referred to the concept of ownership in the section about classification. The *System Owner* is the person responsible for the technical management of a given IT system. It is her responsibility to ensure that the specifications of the Security Framework document and the relevant position papers are implemented and maintained. It is also her responsibility to decide on the classification of the system, should it differ from the default. The name of the System Owner is given in the datasheet for each system and should clearly displayed whenever a user accesses the system and on or near the system itself where it can easily be seen.

## 6. Policy Content

### What position papers should I have and what should I say in them?

Now that you have this fabulous framework within which to structure your policies you may be wondering just what you should say in them. Now, I know you must be tiring of me saying this,

but the honest answer is that I really don't know. Your policies must be based on the real requirements identified by the security risk assessment you performed. But everyone loves a shortcut, so here are two:

## 6.1 Some things each position paper should say

In each paper that forms part of your policy paper you should include at least the points listed below. You could even use these points to create the structure of your position documents:

1. **Scope:**  
Precisely what issue, organizational unit or technological system that the paper cover.
2. **Validity:**  
Each policy should have a limited life span and be reviewed on a regular basis.
3. **Ownership:**  
A name and contact details for the 'owner' of the document, as described earlier in this paper.
4. **Responsibilities:**  
A description of who is responsible for which elements of the security of the system or issue being covered. This is important if one wants to enforce accountability.
5. **Supporting Documentation:**  
A reference to other documents higher or lower in the policy structure, for example, the *Security Framework* document or a specific *Technical Guide*.
6. **Position Statement:**  
What you actually want to say about the issue (kind of the hard part).
7. **Review:**  
Whether, when and how security reviews will be performed on the systems in question.
8. **Compliance:**  
A statement regarding the consequences of non-compliance with the policy.

## 6.2 Policies for free

There are a number of good examples of policies to be found on the web, both for free and at a price. One excellent resource for position papers is Mr Charles Cresson Woods' comprehensive book - "*Information Security Policies Made Easy*", which is available from Baseline Software <<http://www.baselinesoft.com>>. Although my feeling is that Mr Cresson Woods' policies are (for the most part) too generic, his book can give you an idea of what should be covered and there definitely are some policies that can be used. The book comes with a CD that has the policies in electronic format for easy copy-and-pasting.

## 7. Assessing Policies

How do I ensure policies have an impact on my organization?

If the security process at your organization is nearing its end, or if you already have a system of security policies in place, then you may be asking yourself whether or not the policies you've defined are actually having any impact on your organization. The proper way to do this is of course via another risk assessment exercise, thus completing the security cycle. But you may be able to do a snap assessment of your policies without having to go through the entire risk assessment process.

Here's a list of simple questions you can ask yourself whilst reading policy documents to get an idea of how effective they'll be in your organization:

1. Does the policy have a clearly defined **scope**? Is it clear to which system and which people the policy is applicable?
2. Is the policy **comprehensive** in terms of the defined scope it means to address? Are all systems and issues sufficiently covered?
3. Does the policy clearly define **responsibilities**? Is it clear to the end-user, the line-manager and the various administrators exactly what his or her responsibilities are? Is it clear who is responsible for various aspects of security?
4. Is the policy **enforceable**? Can it be applied in a concrete manner so that the compliance is measurable?
5. Is the policy **adaptable**? Can it be easily changed to address new risks and new technologies?
6. Is the policy making an **impact**? Is the policy well distributed, is there an awareness of the policy and is its content understood?

These are typically also the questions auditors and security analysts will be asking themselves as they review your security mechanisms.

## 8. Global Best Practice

### Measuring your policies against international standards.

At least one good reason to have security policies is to prove to the world that your organization is taking all reasonable steps to ensure the confidentiality and integrity of its information assets. This is of course particularly important for publicly listed companies, for companies in the process of mergers and acquisitions and for companies seeking investors and business partnerships.

According to the SANS institute ([www.sans.org](http://www.sans.org)), a major trend in IT security this year will be that large organizations will require their e-business partners to comply with a set of operating regulations that ensure that appropriate levels of security are maintained. For example, industry leaders like VISA have already begun this process with their partners.

What are "appropriate levels of security" then? A Security Standard contains a list of required controls that need to be in place to ensure appropriate levels of security. When an organization has effectively implemented the controls prescribed by the standard it can apply for 'Certification' to the Standard from the Standard's governing body.

One Standard doing the rounds in the 'buzz word crowd' is *BS 7799*. Issued by the British Standards Institute (BSI) in the United Kingdom, this Standard is likely also to become incorporated into the ISO standard set. *BS 7799* comprises 137 control objectives to be achieved before an organization can apply for Certification to the Standard.

Implemented properly, standards like *BS 7799* can significantly further your organization's IT security objectives, but be aware that this is not the only available security standard today. It is important for an organization embarking on the long and hard (and expensive!) route to

certification to understand what the envisaged security standard will offer them and their business partners in the long run.

If you are considering structuring your policies within the framework of a security standard like BS7799 then here are some questions you can ask to help you decide:

## **8.1 Recognition**

If a major purpose of certification is to assure customers of your security readiness then the certification chosen must be highly regarded by your target market – basically the people you are trying to impress. This is possibly the single most important factor.

## **8.2 Focus**

The various certification programs tend to focus on different aspects of IT security. For example, GMITS takes a business-oriented approach whilst ITSEC tends to focus on technology. A certification path needs to be chosen that is compatible with your organization's own security objectives.

## **8.3 Local presence**

Apart from the standards body itself the process of certification typically requires the participation of two other parties – the process consultant who will lead you through to certification and the assessors who make the certification approval. You must determine if the correct people are available to be in your country or state to do this work. This is of course particularly important for the BSI standards.

## **8.4 Cost**

The cost of the certification must be weighed up against the value it offers.

## **8.5 Endurance**

The certification process should have long-term benefits that outweigh the costs. This means:

1. The effects of the process should be practically tangible (the systems should be more secure afterward)
2. The process should not have to be repeated too often.

## **8.6 Objectivity**

It is generally not a good idea to be officially audited by companies that also sell security products. However, this is not a black-and-white issue and most security companies today offer both services and products successfully.

## **8.7 Conclusion**

Security standards are a form of globally recognized security benchmarking that offers numerous business and technological advantages. However, it should be emphasized again that security certification is a long and difficult process. You'll want to carefully consider the value gained by this in relation to the costs involved.

## 9. Examples

### 9.1 An IP network security policy

This section contains an example of a position paper for an IP network for a fictitious company called “Foobar”. The policy documented here makes extensive use of the system of classification explained in earlier in this paper. You should ensure that they understand this system before continuing.

#### 9.1.1 *Issue Statement*

The intent of this policy is to ensure that all systems installed on the Foobar network are maintained at appropriate levels of security while at the same time not impeding the ability of Foobar users and support staff to perform their work. The purpose is:

- To define **where** equipment is to be placed on the network.
- To define **who** may access network equipment.
- To define **how** access to this equipment is to be controlled.
- To define how data **traveling** over the network is to be protected.

#### 9.1.2 *Applicability*

This policy applies to:

- any IP networks (existing and future) to which FOOBAR network equipment is connected
- all equipment connected to the networks mentioned above
- any IP networks across which Foobar data travels
- data in transit over any of the above-mentioned networks
- network administrators managing the equipment
- project leaders requiring new equipment to be connected to the network
- all users utilizing equipment that is connected to the network

This includes, but is not limited to:

- The **User LAN** – 2.3.4.0/24
- The **SERVER LAN** – 2.3.5.0/26
- The **Backup SERVER LAN** – 2.3.5.64/26
- All **backbone** services, Switches, ADSL, Internal Dial-Up etc
- **Remote Sites**

All equipment to the networks mentioned above and all Foobar employees using any of this equipment are also covered by this policy.

### 9.1.3 Statement of Foobar's Position

#### General

This policy is based on the principles and guidelines described in the Foobar Corporate *Information Security Framework* document.

All Foobar network equipment (routers, servers, workstations etc) shall be classified according to the standard Foobar classification and placed in a network segment appropriate to its level of classification and access to these segments must be controlled in an appropriate manner. Whenever data travels over a network segmentation of a lower security classification then the data shall be protected in manner appropriate to its classification level.

#### Classification

1. In accordance with the Foobar Corporate Security Framework all users, hosts and data must be classified as *Security Level 1, 2, 3 or 4 (1 - Unclassified, 2 - Shared, 3 – Company Only or 4 – Confidential)*. All physical network segments, IP subnets and other IP traffic carriers must be classified in the same way. All data traveling on an IP network must be classified and all users accessing network equipment or requesting data over the network must be assigned a level of clearance according to the same system.
2. It is the function of the *equipment owner* to have all equipment under his or her control classified. The *owner* is defined as the head of division installing the equipment. Classification is done in consultation between the owner (or an assigned representative) and the Security Officer but the final decision shall lie with the Security Officer.

For a definition description of the Foobar system of security level classification, the concept of *ownership* and the role of the *Security Manager* refer to the Foobar Corporate Information Security Policy Framework.

#### Network Segmentation

1. Unless otherwise stated in this document all network segments are classified **Level 1 – Unclassified**.
2. The classification of network segments is given in the *Classification* section, later in this document.
3. A network segment can only be classified as another security level with approval of the Foobar Security Manager. Its new level of classification must be recorded in this document and all divisional heads must be notified.
4. Wherever a network segment connects to another network segment of a different security level, then the connection between the two networks must be controlled by an approved *Trusted Point*. A 'Trusted Point' is equipment capable of regulating the flow of traffic between two network segments in a manner appropriate to the classification of the networks. Trusted points are covered in detail in the section that follows.

5. No network equipment may be connected to a network segment that is not of the same security level as the equipment itself.
6. The Foobar Security Officer may also choose to segment two networks of the same security level.

### Trusted Points

1. The trusted point used to segment two networks shall be appropriate for the network with the highest security level.
2. The default behavior of a trusted point must be to deny all IP traffic between the network segments it protects.
3. On the discretion of the Foobar Security Manager the default behavior of the trusted point may be to allow all traffic out from the network with the higher security level whilst denying all traffic in.
4. On the discretion of the Foobar Security Manager the trusted point may be configured to allow specific into the network with the higher security level.
5. All trusted points must be completely under the control of the Security Manager. Access to any trusted point shall only be with the explicit permission of the Security Manager and under his or her close supervision.
6. There are a number of technologies that can act as trusted points. They're divided into the following categories:
  - **Network Level Control:** TCP wrappers, *host.allow* lists, filter routers, network-level firewalls, V-LAN switches etc.
  - **User Level Control:** Application proxies, user-level firewalls etc
  - **Strong User-Level Control:** Token based user authentication systems, certificates etc
7. Whenever there is a connection that skips over one security level then strong user level control must be used. Even if strong user control is used, a connection may never skip more than one security level.
8. Control of traffic must be exercised in the manner listed below:

For connections <i>into</i> <b>Unclassified</b> classified segments		
From	Control Type	Comment
Unclassified	No controls	
Shared	No controls	
Company Only	No controls	<i>With the exception of the Internet</i>
Confidential	No controls	
For connections <i>into</i> <b>Shared</b> classified segments		
From	Control Type	Comment
Unclassified	No controls	
Shared	No controls	
Company Only	No controls	

Confidential	No controls	
<b>For connections into <i>Company Only</i> classified segments</b>		
From	Control Type	Comment
Unclassified	<u>Via a proxy</u> : Network level control to and from the proxy. Direct: Strong user-level control	<i>This allows both for things like incoming SMTP and user dial-in.</i>
Shared	Network level control	
Company Only	No controls	
Confidential	No controls	

<b>For connections into <i>Confidential</i> classified segments</b>		
From	Control Type	Comment
Unclassified	Not permitted	
Shared	Not permitted	
Company Only	Strong user-level control	
Confidential	No Control	

#### Data in transit

1. Data moving on the network between any two network-components is considered *data in transit*. This also includes all control and management sessions.
2. All network technologies are regarded as either *safe* or *unsafe* in their native state (i.e. without any encryption). The only networks regarded as *safe* by Foobar are Frame-Relay PVCs (as used on the Foobar backbone) and switched Ethernet LANs. All other network types are regarded *unsafe*.
3. All data in transit over an *unsafe* network segment that has a classification lower than the classification of the data must be protected by data encryption. Data in transit over a *safe* network segment may be encrypted at the discretion of the Security Officer.
4. Encryption of data in transit may take any of the following forms:
  - *Network encryption*, where data is encrypted at the IP layer (e.g. IPSec)
  - *Session Encryption*, where data is encrypted at a TCP layer (eg SSL)
  - *Message encryption*, where blocks of data are encrypted before they are sent (eg SMIME)
  - *Data encryption*, where the entire data package is encrypted for it is transmitted (eg file encryption)
5. Encryption systems used must offer strong encryption (more than 100 bit encryption keys) and use Internationally recognized encryption algorithms. The choice of the crypto-algorithm is the responsibility of the Security Officer and is laid out in Foobar's position paper on Cryptography.

#### Internet

Access to the Internet from Foobar networks is considered a special case and is dealt with as an issue on its own in the Position Paper on Internet Access.

#### 9.1.4 Classifications

##### Users

1. Every user is cleared as *unclassified* until his or her classification is explicitly changed with the written approval of the Security Officer.
2. When a new employee joins Foobar, a request is made by the employee's manager to the Security Officer for a new level of clearance. It is the responsibility of the manager to justify the requested level of clearance.
3. Unless there is strong justification all new employees shall be cleared for the level *Foobar Only*, but only after they have signed an employment contract including acceptance of this policy and non-disclosure forms.
4. The Security Officer is responsible for managing and controlling the record of clearance levels for all personnel.
5. It is the responsibility of all system owners and system administrators to determine the security level of a given user before granting that user access to any system.
6. It is the responsibility of the user to know his or her own clearance level and to understand the rights and limitations associated with that clearance.

##### Equipment

1. All computing equipment must be given a classification by the Foobar Security Officer.
2. Classifications for existing Foobar equipment are listed below:
  - All user workstations, file-servers, print-servers etc are classified as **Company Only**,
  - All SERVER LAN servers and other hosts used in the management of the Foobar backbone infrastructure or Foobar internal network infrastructure are classified as **Confidential**.
  - All backbone equipment (including switches, remote access servers, ADSL chassis etc) not located on Foobar premises are classified **Shared**.
  - All equipment used in the transfer of data to and from the Internet is classified **Shared**.
3. The Security Officer must maintain a complete list of the classifications of all computing equipment in the Foobar network and in the Foobar backbone.

##### Networks

1. The Foobar Security Officer must classify every network segment forming part of the Foobar infrastructure.
2. Classifications for existing Foobar network segments are listed below:

- The Foobar User LAN located is classified as **Company Only**.
  - The SERVER LAN & backup SERVER LAN are classified as **Confidential**.
  - The Foobar Frame-Relay Backbone is classified as **Shared**.
  - The Remote sites are classified as **Shared**.
  - The SERVER LAN and the Portal Segment are classified as **Shared**.
3. A complete list of the classifications of all network segments in the Foobar network and in the Foobar backbone is maintained by the Security Officer.

### Physical Locations

1. The Foobar Security Officer must classify every network segment forming part of the Foobar infrastructure.
2. Classifications for existing Foobar network segments are listed below:
  - The Foobar User LAN located is classified as **Company Only**.
  - The SERVER LAN & backup SERVER LAN are classified as **Confidential**.
  - The Foobar Frame-Relay Backbone is classified as **Shared**.
  - The Remote sites are classified as **Shared**.
  - The SERVER LAN and the Portal Segment are classified as **Shared**.
3. The Security Officer must maintain a complete list of the classifications of all physical locations in Foobar.

### Data

1. Any Foobar user with legitimate access to Foobar data may, with sufficient justification, change the classification of the data. The user may only change the classification of data if there is sufficient, justifiable reason to do so. Users will be held strictly responsible for these decisions.
2. Classifications for existing Foobar data are given below:
  - Foobar business information (memos, financial documents, planning documents etc) should be classified as **Company Only**.
  - Foobar customer data (contact details, contracts, billing information etc) should be classified as **Company Only**.
  - Network Management data (IP addresses, passwords, configuration files etc) should be classified as **Confidential**.
  - Human resources information (employment contracts, salary information etc) should be classified **Confidential**.

- Published information (pamphlets, performance reports, marketing material etc) should be classified **Shared**.
  - Email between Foobar employees should be classified **Foobar Only**.
  - Email between Foobar employees and non-Foobar employees should be regarded as **Unclassified**.
3. All newly created data must be classified **Company Only** until it is reclassified by a user, who does so at his or her own prerogative.
4. Users are held solely responsible for any data that's classification they change.

### 9.1.5 Roles and Responsibilities

1. It is the responsibility of the **user**:
  - to know his or her own clearance level and to understand the rights and limitations associated with that clearance
  - to ensure all the data he or she works with is correctly classified
  - to ensure that he or she understands the restrictions associated with the data he or she is working with
  - to ensure all the data he or she works with is housed and protected appropriately
2. It is the responsibility of all system owners and system **administrators**:
  - to determine the security level of a given user before granting that user access to any system
  - to verify the classification of the equipment they manage
  - to verify that the equipment is installed and protected in accordance with its classification
3. It is the responsibility of each divisional **manager**:
  - to obtain clearance for employees in his or her divisions
  - to clarify the classification of data on systems under his or her control
  - to clarify the classification of equipment under his or her control and to ensure that those systems are correctly installed
  - to ensure all employees in that division understand and implement this policy
4. It is the responsibility of the **Security Officer**:
  - to approve all classifications
  - to maintain a list of all classifications
  - to approve the final layout of the Foobar network and backbone
  - to control and manage all trusted points
  - to determine the type of cryptographic protection to be used for data in transit

### 9.1.6 Compliance

1. Any user accessing a data, equipment or a physical location with insufficient clearance can face disciplinary action, dismissal and criminal or civil prosecution.
2. Any user allowing access to a system that he or she controls for someone with insufficient clearance can face disciplinary action, dismissal and criminal or civil prosecution.
3. Any person connecting equipment that is not classified to the network or connecting equipment to an inappropriate part of the network or in an inappropriate location can face disciplinary action, dismissal and criminal or civil prosecution.
4. Any person transmitting data over any network without the appropriate cryptographic protection for that data can face disciplinary action, dismissal and criminal or civil prosecution.
5. Any person changing the classification of data in a way that is reckless, irresponsible or in any damaging to Foobar, their share holders or any of their clients can face disciplinary action, dismissal and criminal or civil prosecution.

### 9.1.7 Points of Contact and Supplementary Information

1. For a description of the Foobar system of security level classification refer to the Foobar Corporate *Information Security Framework*
2. For contact details for the *Foobar Security Officer* refer to ...

For enquiries regarding the classification of data, equipment, network segments or physical locations or the clearance level of users contact the Foobar Security Officer.

## 10. Conclusion

This has been a very long paper and a lot was said. Let me try to summarize the important points should remain stuck in your mind:

1. If policies are properly implemented they can become an effective and efficient part of your information security arsenal. Because policies secure the 'human element' they address an element of your risk profile that is seldom touched by technology.
2. There are no silver bullets in security and the same is also true for information security policies. Your policies should be written to counter your specific risk profile and should be based on the findings of a security risk analysis exercise.
3. Policies can only be effective in a corporate environment that prioritizes security as a goal. It may be necessary to make some far-reaching changes to your organizational structure and culture before policies can have an impact and your security objectives can be achieved. Foremost among these changes is the designation of responsibility and the commitment of funds.
4. Your policies must be designed 'for the people' and be easy to access, use and understand. To facilitate this I suggest that the documents be structured in a hierarchical fashion with documents having different levels of detail. Responsibility for the management of this document tree should be specifically assigned.
5. Although the actual content of policy documents should vary radically from organization to organization but there are some fundamental principles that each policy should enforce.

Once your policies have been implemented you will have a structured, formal framework to guide your security strategy and according to which the progress of process can be measured.

## **11. References**

[1] Snow, Dick; Department of Computing Science, University of Newcastle upon Tyne; "Security Models"