



**Why**

**Information Ownership**

**for**

**Managers?**

**Peter Wood**  
First • Base  
Technologies



### What is information ownership?

The concept of information ownership is simple – if you use information in your day-to-day work, then you should be responsible for it.

### What does this responsibility entail?

Suppose you write a report following a member of staff's annual review. This report is obviously confidential to some degree – it should only be viewed by a select group of people.

Since you created the report, this makes you the *information owner*. As the information owner, you are responsible for protecting this document to an appropriate degree.

### What types of protection are there?

#### Confidentiality

This means that you should ensure that only the appropriate people get to see the document. To achieve this, you would need to make a list of who should be allowed to see the document, then somehow ensure that only these people *can* see the document.

If the document is to be stored in a large computer system, you would need to ask the IT department to secure it for you (this makes IT the *information custodian*). However, it still falls to you to give them the list of people who are allowed to see the document.

If the document is to be stored on a laptop, then you become both the information owner and information custodian. It is your responsibility to guard access to the laptop, in order to protect the information stored on it.

You must also consider where the printed document is to be stored – there is no point in protecting the information on the computer if someone can walk up to your desk and simply read the paper copy!

## Why Information Ownership for Managers?



### **Integrity**

Integrity means that you should ensure that only the appropriate people can change the contents of the document. Again, you would need to make a list – this time of who should be allowed to *alter* the document.

As before, if the document is to be stored in a large computer system, you would need to ask the IT department to secure it for you (this makes IT the *information custodian*). However, it still falls to you to give them the list of people who are allowed to *change* the document.

Of course, if the document is to be stored on a laptop, then you again become both the information owner and information custodian.

### **Availability**

Availability is about ensuring that the information is there when you (or the other users of the information) need it.

Typically if the document is stored in a large computer system, the IT department ensures that the necessary backups are taken, that the systems are protected against electricity failure, and that the equipment receives regular maintenance.

However, if the document is to be stored on your laptop, then again you become both the information owner and information custodian. It is your responsibility to back up the file regularly in case your laptop fails. You may simply keep a printed copy of the document as a backup, or you may take copies of the information onto floppy disk.

### **Which information should I protect?**

One of your most important tasks will be to categorise the information you own. (*information classification*)

This need not be a laborious task. You probably already know which information is sensitive, which company confidential, and so on.

## Why Information Ownership for Managers?



The key is to label the information in a simply and quick fashion, so that you know how to treat it, and so do your staff and your IT department.

Guidelines on information classification will be issued along with your training on this important topic.



### Definitions

#### Information owner

The most senior person responsible for the security of the information asset, usually a manager or senior manager.

It is this person's responsibility to:

1. determine which information is sensitive, valuable or critical and create an inventory of that information
2. allocate a degree of confidentiality, integrity and availability to that information (*information classification*)
3. liaise with the information custodian for each information item to ensure that the appropriate degree of protection is assigned to that information
4. sponsor regular reviews of the information inventory
5. sponsor regular audits of the protection accorded to the information

#### Information custodian

The person responsible for implementing the security of the information asset, as defined by the Information Owner. This may be someone controlling access to a computer system, a specific application program or even a filing cabinet.

#### Information user

The person responsible for the amending the content of the information asset. This is any user of the information in the inventory created by the Information Owner.

#### Line manager

The person responsible for managing the information users.



### Example Summary of Actions for Information Owners

1. Identify valuable, sensitive or critical information assets and create an inventory of them.
2. Classify the information assets in terms of Confidentiality, Integrity and Availability.
3. Request the Information Custodian to secure the information assets in an appropriate manner for the asset's classification.
4. Ensure that the logon controls and access permissions applied by the Information Custodian provide the required levels of confidentiality.
5. Each month, request a list of user logons for each information asset from the Information Custodian. Compare this list with the current known users and request the Information Custodian to suspend or remove any redundant user logons.
6. Ensure that no users have unique skills relevant to the information assets. If any such users exist, ensure that at least one other user is trained to act as a backup.
7. If confidential or sensitive output may be sent to a printer, ensure that it is located where the output cannot be seen by inappropriate staff.