



## Asset identification

This is a list of some types of assets. The list is not exhaustive.

### Physical assets

- computer and communications equipment (owned by MIS)
- magnetic media (owned by Manager)
- power supplies and plant, such as air-conditioning units (owned by MIS)

### Software assets (owned by MIS)

- application software
- system software
- development tools
- utilities

### Information assets (owned by Manager or MIS)

*'Information' means information held by the Company on its own behalf and that entrusted to it by others. The following are examples of the media which may contain or comprise information assets.*

- databases and data files
- system documentation
- user manuals
- training material
- operational or support procedures
- continuity plans and fallback arrangements
- back-up media
- on-line magnetic media
- off-line magnetic media
- paper

### Services

- computing and communications services (owned by MIS)
- heating, lighting and power (owned by Manager or Building Services Manager)



## Categories for classifying document security

### Category 1 : Routine (non-confidential) documents

**Description:**

All documents of a routine nature.

**Effects of disclosure:**

No measurable damage to the company or a department.

**Examples:**

Normal memos, routine reports, circulars.

**Estimated occurrence of this classification:**

More than 80% of all documents would be within this class.

**Recommended marking of document:**

This is the default class. Therefore, there should be no need to mark non-confidential material, and all unmarked material would normally be expected to fall in this category.

**Recommended electronic storage:**

On network drives including shared areas without concern. Laptop users may store such documents on their local hard drive.

**Recommended paper storage:**

Normal filing systems even where cupboards and offices are insecure.

**Recommended electronic distribution:**

Electronic mail or conferencing software, or via shared drives or document management systems.

**Recommended physical distribution:**

Unsealed re-usable envelopes through the internal post. Normal mail for external posting.

**Recommended disposal:**

Paper documents should be placed in office waste paper baskets or recycling bins.

Electronic mail messages may be freely deleted.

Files may be deleted from local or network disks without precaution.



### Category 2 : Confidential (or "Personal")

**Description:**

Any document where the information should not be distributed freely. NB the only difference between Confidential and Personal lies in the nature of the contents, confidential material relates to the business, personal material relates to the individual - they should be treated in an identical fashion.

**Effects of disclosure:**

Some embarrassment or difficulty may arise or a breach of professional etiquette may be involved (e.g. in handling personnel data), but where no serious damage to the company or its brand or the dignity of its employees would result.

**Examples:**

Confidential: Planning documents; much personnel data (excluding salary data which should always be Strictly Confidential); drafts of important papers prior to their publication; supplier or customer documents marked confidential.

Personal: Invitations to retirement functions, notes of greeting or condolence.

**Estimated occurrence of this classification:**

Less than 10-20% of the total documentation

**Recommended marking of document:**

Document (and envelope) should be marked "Confidential" (or "Personal"). Report or spreadsheet headings should be similarly annotated.

**Recommended electronic storage:**

On a password protected network drive (e.g. drive H:\), or for a workgroup a private shared area on a network server.

**Recommended paper storage:**

In locked drawer or cupboard.

**Recommended electronic distribution:**

Electronic mail would normally be considered secure enough for this data. NB some senior managers do permit their secretaries to access their mail. Where this is a possibility, the subject field should contain the word "Confidential" (or "Personal"). A private shared network drive would also be acceptable. Portable users should only use their local hard drive where they have a secure laptop PC with implementations of power-on passwords and password protected screen savers.

**Recommended physical distribution:**

In sealed envelope clearly marked "Confidential" (or "Personal"). NB some senior managers instruct their secretaries to open this category of mail, but the responsibility for the security of it remains with that manager.



### **Recommended disposal:**

Paper documents should be shredded.

Electronic mail messages should be deleted, and the electronic wastebasket checked to ensure that no copy is accidentally retained there.

Files can be deleted from the networked disks without further precaution. Files held on a local hard disk may be safely deleted if they are encrypted or password protected.

Consideration should be given to retaining all types of material that will lose its confidentiality with age. Then it may be simply destroyed in a non-confidential manner.



### Category 3 : Strictly Confidential

**Description:**

Any document where disclosure would cause actual or potential harm or severe embarrassment.

**Effects of disclosure:**

Damage to company image or staff morale. Loss of competitive advantage. Serious breach of professional etiquette, e.g. disclosure of medical records or salary data.

**Examples:**

Sales plans, sales margins, new stores and product launches. Salary reviews, staff appraisals. Medical centre records. Re-organisations.

**Estimated occurrence of this classification:**

Much less than 5% of total documents (probably less than 1%).

**Recommended marking of document:**

Document (and envelope) should be marked "Strictly Confidential". Report or spreadsheet headings should be similarly annotated.

**Recommended electronic storage:**

Where possible (i.e. Word, Excel etc.) the document should be password protected. Consider the use of encryption software where users are PC literate. Consider storing on diskette but a backup copy must be made as well.

**Recommended paper storage:**

In secure locked cupboards, with no hidden keys left within the office.

**Recommended electronic distribution:**

Where necessary, this should be achieved by sending password protected or encrypted documents. Passwords to be selected to be difficult to crack. Passwords must not be sent electronically.

**Recommended physical distribution:**

Sealed envelopes handed to the recipient wherever possible. Where internal post has to be used, all envelopes should bear an "Only to be opened by" sticker. Secretaries to be instructed to hand envelope to managers unopened.

**Recommended disposal:**

Paper documents should be shredded.

Files can be deleted from the networked disks without further precaution. Files held on a local hard disk may be safely deleted if they are encrypted or password protected. Diskettes should be reformatted or physically destroyed.

## Guidance on Information Classification



Consideration should be given to retaining all types of material that will lose its confidentiality with age. Then it may be simply destroyed in a non-confidential manner.



### Category 4 : Secret

**Description:**

Documents of the utmost importance to the company.

**Effects of disclosure:**

Severe damage to the company fortunes or image will result.

**Examples:**

Acquisitions, divestments, major company re-organisations.

**Estimated occurrence of this classification:**

Extremely small 0.01% or less of total documentation.

**Recommended marking of document:**

Document (and envelope) should be marked "Secret". Report or spreadsheet headings should be similarly annotated.

**Recommended electronic storage:**

Not recommended but if essential on diskette stored in a safe, or on the local hard disk of a stand alone PC unconnected to network. Encryption should be used and PC should be in secure locked room.

**Recommended paper storage:**

Locked in a safe.

**Recommended electronic distribution:**

Not recommended.

**Recommended physical distribution:**

In sealed envelope handed to addressee or sent by registered post or secure courier.

**Recommended disposal:**

Paper documents should be shredded in high quality shredders (on the advice of the company Security Consultant) or should be sent to specialist security disposers under the supervision of the company Security Consultant.

Files on any PC disk or diskette should be irrevocably wiped using proprietary high security disk wiping utilities under the supervision of Network Services' management. Alternatively, diskettes could be physically destroyed.

Consideration should be given to the secure retention of all types of material that will lose its secrecy with age. Then it may be more simply destroyed in a non-confidential manner.



### Risk Assessment Guidelines

#### Vulnerability

The following risks give some idea of the general vulnerabilities that we, as individuals, and the Company as an organisation, are subject to:

- deliberate or accidental damage to property or equipment;
- unauthorised removal of personal property, company property or information;
- actions of terrorist or antagonist groups in disrupting business.

Information forms a major element of the Company's business and if it falls into the wrong hands this could have far reaching effects on the integrity, confidence in and commercial viability of the Company. All staff must therefore regard all Company information as being sensitive and make sure that they do not disclose it to anybody unless they are certain that the person has a right to it. In case of doubt staff members should refer requests for information to their immediate supervisor.

All staff members should be aware of the type of risks that we might be vulnerable to; for example:

- theft and exploitation of sensitive information and documents. This may be done in order to gain financial advantage, or for other, less obvious reasons;
- loss of documents inside the Company or outside at meetings or when travelling;
- intentional or unintentional disclosure of sensitive information to agencies such as the press or agencies seeking to make profit. Accidental disclosure can take the form of careless talk in places such as lifts, wine bars, trains, etc.;
- careless behaviour or action, such as leaving sensitive information in general areas, leaving discarded copies in waste bins or papers in photocopiers;
- interfering with computer software or data; for example by "hacking" into the Company's systems;
- deliberate destruction of computer programs;
- overhearing conversations in open offices or over telephones;
- allowing visitors or non-authorised staff to enter controlled areas;



- subversion of staff through bribery or blackmail;
- fire and other destructive mechanisms.

It is possible that many small pieces of information can be assembled, much like a jigsaw puzzle, to provide the determined “agent” with a comprehensive and perhaps highly damaging picture with which to operate against or profit from the Company. The disclosure of any information outside the Company must therefore be guarded against.

### Assessment guidelines

The magnitude of a risk depends upon the probability of the threat and the impact. Impact in turn depends upon the value of the asset at risk (i.e. how much damage might be done) and its vulnerability (e.g. An office building is very valuable. It could cost millions of pounds to replace. It may be vulnerable to fire, explosion or even earthquake. It is far less likely to be stolen.)

There are three main categories of vulnerability:

- **confidentiality** - the value that comes from an information asset being not generally available outside of the business, which can be impaired if the information is made available to others in an uncontrolled manner;
- **integrity** - which may be considered to be fitness for purpose, an asset is functioning correctly, information is complete, accurate and as up to date as expected;
- **availability** - the need to have an asset available when required by the business;

These vulnerabilities can be further subdivided between accidental and deliberate. In some cases the impact is unaltered (it makes very little difference to the business whether an asset which is needed is destroyed accidentally or deliberately) but it can make a considerable difference to the controls needed to prevent, detect or control the risk.

If the prime vulnerability is because of accidental threats, controls which guard against deliberate threats may not be so important. Care should, however, be taken. If an asset is not protected against deliberate threats, legitimate users may see this as an indication that the asset is not of value and become careless.

### Assessing confidentiality requirements

How much damage to the Company or its business interests could be caused by loss of confidentiality of the information (e.g. information is accidentally or deliberately made known to individuals or the public)?



- Low** Very little damage - the information is public or of little value to a competitor. Anyone may read the information if they wish.
- Medium** Some damage - the information could cause some embarrassment if made public. There might be some advantage lost to the Company or a party who entrusted information to the Company if the information were known by competitors. There are laws or contractual agreements requiring reasonable confidentiality measures (e.g. the Data Protection Act) but the information is not highly sensitive.
- High** Significant damage - the information would be highly embarrassing if made public or there would be significant advantage lost to the Company, or a party who has entrusted information to the Company, if the information were known by competitors. There are laws or contractual agreements requiring reasonable confidentiality measures and the data is sensitive.

### Assessing integrity requirements

How much damage to the Company or its business interests could be caused by an impairment to the integrity of the asset (e.g. equipment which appears to be operating correctly when it isn't, information which appears to be correct when it is inaccurate)?

- Low** Very little damage - little change of any significant defect going unnoticed, information is treated as indicative or aide memoir.
- Medium** Some damage - could result in lost business, information is relied upon in making important business decisions.
- High** Significant damage - visible disruption to the Company, misleading information published, potential to be used for fraud involving significant amounts of money.

### Assessing availability requirements

How much damage to the Company or its business interests could be caused by loss of availability of the asset (e.g. equipment breakdown, destruction or theft - individual unavailable - information unavailable through equipment failure or lost through destruction of media)?

## Guidance on Information Classification



- Low** Very little damage - asset is not easily destroyed or damaged, can be easily replaced, has little chance of theft as realisable value is small compared to the effort of removing - business could continue without the asset or there are similar assets that could be used elsewhere in the Company. Information is readily available elsewhere or could be recreated at little costs.
- Medium** Some damage - asset would have to be replaced at a reasonable cost and reasonably quickly. Business would be significantly less efficient or effective if the asset was not available for more than 1 business day.
- High** Significant damage - visible disruption to Company business. Bad publicity likely if the asset is not available for more than a few minutes at a key time. Asset is small, valuable and easily disposed of for cash (e.g. computer chips).