Introduction

Data classification and allocation of responsibilities for its ownership are important to ensure that the value of information is properly recognised. It is the first step towards ensuring that the most valuable information assets have the highest level of protection.

Information varies in its degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. The information classification scheme should be used to define an appropriate set of protection levels, and communicate the need for specialising handling measures.

What is data (or information)?

The terms 'information' and 'data' are used interchangeably throughout this document.

Information can be defined as … any communication or information such as facts, data, or opinion, whether true or not, whether recorded in a material form or not, whether numerical, graphic or narrative, and whether maintained in any medium, including computerised databases, paper, microform, optical disk or magnetic tape.

Examples… Customer information – payment history, personal history, pricing information for particular customers

Financial Information – performance history, projections, strong and weak points

Other Confidential Business Information – business allies, specific projects, employeerelated problems, management-problems, marketing information, expansion, contraction, target markets, hiring, takeover targets, new products/services, inventions and discoveries

Why do we (or must we) care?

We have a duty to protect the security of, access to, correction of, use of, and disclosure of data – often because it is a matter of law. A growing number of legislative mandates are appearing in the area of information security. Although these cover a variety of issues (computer misuse, etc) the area attracting most attention is that of Data Protection.

Classification Levels

By classifying information, the correct level of protection will be defined and implemented. Information identification should be done at a high level and identify broad categories of information

Here are four classification levels that identify the level of protection that should be given: Public (Class 1) - Non-sensitive information available for external release ·

Internal (Class 2) - information that is generally available to employees and approved non-employees

· Confidential (Class 3) - information that is sensitive within the company and is intended for use only by specified groups of employees

· Restricted (Class 4) - information that is extremely sensitive and is intended for use only by named individuals within the company