# Data Classification

One of the biggest issues facing many organisations today, especially Government departments and public bodies is that of Data Classification.

For many in this environment, the true record for archival and reference is the paper one, the electronic version of the document does not get the same level of attention from a security perspective.

Data Classification is the assignment of a level of sensitivity to a specific piece of information. This sensitivity is with respect to the impact that unauthorised access to this would create.

For many organisations, this is typically broken into 3 – 5 different ratings from Top Secret to Public Documents.

Only when a piece of information, or a piece of information processing infrastructure has been classified can appropriate security controls be put in place to protect it appropriately.

It is also vitally important to reclassify information as soon as its classification has changed. For instance, the Minister of Finance's Budget details could be considered Top Secret in the weeks coming up to Budget Day, but once the Minister has made their speech, the classification of these documents now changes to being Public Documents. This reclassification is vitally important to the success of any Data Classification process, as the overhead required to maintain a huge volume of information at Top Secret is massive. It also gives the classification process more value in many users eyes as they can see the burden of managing the more onerous classification levels as being appropriate.

One of the problems facing organisations that undertake a Data Classification exercise is the sheer volume of data that needs to be assessed. What is absolutely critical in moving forward with a process is to make it as simple as possible for any user that is creating or modifying a piece of information to classify it. This is where the technology can be of assistance. It is not a huge exercise to create various scripts and macros that integrate with the various office automation tools such as email clients, word processors and spreadsheets. These add-ons can provide a user with a Data Classification request each time they go to save a document or send an email. These add-ons can either set properties or define particular storage areas based on the classification chosen. Guidelines to assist users in the classification of documents can also be supplied at this stage.

Once the tools are in place to support users, it is important to ensure that the Policies and Standards that are in place within the organisation reflect the new classification process, and that the guidelines are being enforced.

It is within the Policies and Standards that the organisations requirements in terms of handling this classified information. For instance, it may be deemed appropriate to send data that is considered Secret or Confidential via an encrypted email, but it may never be acceptable to send a Top Secret piece of information via the Internet.

The role that management, specifically the Risk Management function, and Data Owners within an organisation have to struggle with is that of defining appropriate Data Classification for information stored, created and processed by that organisation. It is then the role of the Information Security team to support management in this process by selecting and recommending appropriate tools to ensure that the Data Classification guidelines can be adhered to.

Areas that also need to be considered when reviewing the appropriate data handling and data transport guidelines for classified information include the use of remote access and laptops (and other portable computing devices such as Smartphones, Personal Digital Assistants and hybrids such as the Blackberry devices).

The classification process is not an easy one, but is a necessary one, particularly as we move more aggressively to the area of more integrated eGovernment.