An Roinn Airgeadais
Department of Finance

Sráid Mhuirfean Uacht,
Baile Átha Cliath 2,
Éire.

Upper Merrion Street,
Dublin 2,
Ireland.

Teileafón / Telephone: 353-1 676 7571
Facsuimher/ Facsimile: 353-1 678 9936
Glao Áitiúil / LoCall: 1890 66 10 10
http://www.irlgov.ie/finance

E159/29/07

14 December 2007

To all Accounting Officers

Circular 39/07: Classification of material as "top secret"

A Dhuine Uasail

I am directed by the Minister for Finance to refer to Circular 20/98 concerning the classification of material as "top secret" and to say that Circular 20/98 is now superseded by this Circular.

1. Classifying Top Secret Material

The responsibility for classifying material as "top secret" lies with the Department[1] in which the material originated or was initially received. In determining whether information, documentation (including images, audio, video, web content etc), data, knowledge etc. is to be classified as "top secret", Departments need to consider if the release of the material would –

- Put at risk the life or safety of any individual;
- Pose a serious threat to the security, defence or international relations of the State;
- Undermine the policing or judicial or other processes involved in dealing with serious crime;
- Pose a serious threat to the economic interests of the State;
- Adversely affect developments in relation to Northern Ireland.

[1] For "Department" read "Department or Office" throughout this circular.

The classification of “top secret” should be applied only where essential. Excessive usage of “top secret” is likely to debase the classification and lessen its effectiveness. Limited usage of the classification will also serve to underline the truly exceptional nature of the material so classified.

Departments should ensure that documents derived from such “top secret” material e.g. excerpts, paraphrases, summaries, references are similarly classified, where appropriate.

2. Protection of “top secret” information

It is important that where material is classified as "top secret", particular measures are taken to ensure its protection. Where material would not warrant special protection, by definition it should not be classified as "top secret".

It is not possible to be prescriptive about the manner in which Departments should protect information deemed to be "top secret". Arrangements will, of necessity, vary both between, and even within, Departments depending on the nature of the material e.g. the reason for its "top secret" classification, the number and grades of individuals who must have access to the material in the course of their work, the incidence of such access, etc. Nonetheless, it is essential that access to top secret documents is restricted to appropriate people.

At minimum the arrangements should encompass the following –

- the storage of material (including removable electronic media) in a locked safe or departmental strong room with access restricted to a limited number of nominated people;

- the maintenance of confidential file indexes and tables of file contents for all “top secret” material;

- the availability of material for consultation only, and under the direction of a nominated officer of senior rank;

- the application of unique identifiers to any copies made so that such copies can be traced back to their original;

- the maintenance of a register of individuals who access any item of such material (including copies), recording the date and time of such access, the date and time of the material’s subsequent return to safe-keeping, and the signature of the officer accessing the material.

This list is not exhaustive and Departments are free to adopt other measures which they deem to be appropriate.

The arrangements deemed appropriate should be fully documented and formally approved by the Secretary General. These arrangements and the classification of material as “top secret” should be reviewed regularly.

3. Use of Computers and Electronic Storage Media

The preparation and storage of "top secret" material on computers poses particular difficulties that Departments must address. For example, because of the way computers typically use storage media, it can be difficult to ensure that a document is completely deleted. It is imperative that Departments put protocols and arrangements in place that take account of these difficulties. In particular, the protocols and arrangements should address –

- the physical security of the computer(s) on which "top secret" documents are created;
- the physical protection of electronic storage media used for the storage of "top secret" documents when not in active use;
- the provision of facilities that limit access to authorised personnel only;
- the need to completely delete documents, including temporary copies maintained by the application or by the operating system;
- the necessity or otherwise for encryption of "top secret" material;
- the indexing of "top secret" documents held electronically;
- the logging of all access to electronic storage media which contain "top secret" documents; and
- the physical destruction and disposal of electronic storage media at end-of-life.

4. Freedom of Information

It should be noted that any requests for a record classified as "top secret" fall to be considered in accordance with the provisions of the Freedom of Information legislation.

Mise, le meas,

Jim Duffy,
Assistant Secretary.