Information Handling Standard

1 Introduction

UCD's administrative information is an important asset and resource. All administrative information is categorised according to appropriate needs for protection, handling and compliance with regulatory requirements.

This handling standard describes the minimum control framework to be applied to information that has been classified by the information owner.

2 Application of Standard

2.1 All **Information Owners** are responsible for ensuring that this procedure is applied within their area of responsibility for all information covered by the Security Statement of Applicability.

2.2 **Individual staff members** are responsible for ensuring that sensitive information they produce is appropriately protected and marked with the appropriate classification.

3 Policy Statement

3.1 All existing administrative data belongs to one of the classifications in section 4. – This means that existing unmarked information may still be Confidential or Strictly Confidential. Information owners may apply classification markings to existing information at their discretion subject to requirements stipulated in the Security Statement of Applicability.

3.2 Where data is not classified according to another category, it is to be handled as per the requirements for controlled data.

Note: Categorising information does not exclude it from consideration for disclosure under Freedom of Information (FOI) or Data Protection legislation.

4 Information Handling Guide

This guide provides a framework for handling UCD's information resources. It defines the required activities for protection of information by classification type.

Note that handling provisions cover information in systems and in physical forms (documents, portable storage media), and that such materials are also subject to the requirements of records policy.

Data Classification	Strictly Confidential	Confidential	Controlled
Physical access	Stored in a locked cabinet at all times when unattended. Systems storing information must be housed in a secure datacentre environment. Documents should not be stored on a PC or laptop unless encrypted.	Printed Information must be locked away when work area is unattended. Must be stored in a locked cabinet outside normal business hours. Computers with access to confidential information must be locked while unattended (using password protected screensaver)	Controlled information must not be stored in public-accessible areas. Placed out of sight (e.g. in a drawer) when work area unattended. In public open areas, information must be locked away when work area is unattended.
Copies and distribution	Must only be available to named UCD Staff and sections on the distribution list. Copies may only be made available to other individuals with the written permission of the document owner. Information may only be printed or photocopied in the presence of an authorised user.	Must only be made available to authorised UCD Staff or 3rd parties who have a formal agreement containing non-disclosure provisions.	Information may be circulated to staff and 3rd parties at the discretion of the information owner.
Physical Transfer (reports or paper documents)	Paper documents must be transferred in a sealed container / envelope which contains a clear indication that the document must be delivered by hand to the named individual.	Paper documents must be transferred in a sealed container / envelope.	Information may be transferred in unsealed internal mail envelopes.
Electronic storage	Must be stored in systems accessible only to specified users authorised by the data owner. Suitable encryption must be used to protect information in any electronic format, such as on a disk or a server.	Must be stored in UCD systems accessible to only specified users and groups authorised by the data owner. Suitable encryption may be used to protect Confidential information on a portable device (e.g. CD or disk) or on a laptop.	Must be stored on UCD systems and approved storage systems (e.g. UCD File shares) Such information should not be encrypted or password protected unless specifically required.
Electronic transfer (e-mail, FTP etc)	Must be encrypted if transferred via a network.	Document based information (e.g. Word or excel documents) Should be password protected or encrypted if transferred via an external network. Structured data within applications must be encrypted on networks outside the server environment.	May be sent via email without additional security measures.

Data Classification	Strictly Confidential	Confidential	Controlled
Destruction of physical media	All Strictly Confidential information must brought directly a shredding facility for cross-cut shredding & disposal. Storage media which have ever handled Strictly Confidential information must be disposed of according to procedures defined by the System Manager.	All Confidential information must be disposed of in the confidential waste bins for cross-cut shredding & disposal. Storage media which have ever handled Confidential information must be disposed of according to procedures defined by the System Manager.	Systems which handle internal information only may be disposed of using normal disposal methods.
Marking	Items corresponding to this classification which are generated within UCD must carry the Must carry a marking "Strictly Confidential- Circulation Limited to Authorised Users", and have a distribution list which is visible on printed and electronic copies of information.	Items corresponding to this classification which are generated within UCD must carry the Marking "Confidential- for Authorised Use only", and this must minimally appear on the first page of printed materials. Externally generated information which has been classified as confidential should be circulated with handling guidelines equivalent to the above specified by the UCD Information Owner.	No Specific Marking required. Markings associated with Confidential and Strictly confidential information are not to be applied.
Reclassification	Reclassification of information to confidential, internal or public is at the discretion of the listed Information Owner, subject to the relevant University policies, and to the obligations placed on the university by statute, contract or other regulation.	Reclassification of information to internal or public is at the discretion of the Information Owner, subject to the relevant University policies and processes (e.g. FOI), and to the obligations placed on the university by statute, contract or other regulation. Reclassification of confidential information to strictly confidential is at the discretion of the information owner.	Internal information to be disclosed or made public is subject to the relevant University policies (e.g. FOI), and to the obligations placed on the university by statute, contract or other regulation. The information owner may reclassify material as public subject to the requirements of these policies. Reclassification of internal information to confidential or higher is at the discretion of the information owner.

Data Classification	Strictly Confidential	Confidential	Controlled
System controls	Information may only be processed on approved UCD systems conforming to the security requirements of the Information Security Officer, and implemented by a System Manager. Systems and applications providing access to confidential information must have appropriate login banners.	Information may only be processed on approved UCD systems conforming to the security requirements of the Information Security Officer, and implemented by a System Manager. Systems and applications providing access to confidential information must have appropriate login banners.	Information may be processed on systems approved for use within the University.

5 Technical Considerations

5.1 Only approved software may be used to encrypt information. Approved encryption software includes Winzip version 9 and later, the password protection and encryption facilities of Office XP and later, Passwordsafe version 1.7.1 and later. Note that encryption should not be used unless discussed with IT Security.

5.2 Only correctly configured and approved email clients which support network encryption may be used to email data rated confidential or above.

5.3 Passwords or encryption keys required to open encrypted files must be supplied to Information Security on request to facilitate virus scanning or policy compliance checks.

5.4 Templates to facilitate the creation of documents with the appropriate markings are available from the Information Security Officer.

5.5 Contact Information Security on security@ucd.ie for technical advice or if you are unsure about any aspect of this procedure.