Dublin City University

Data Handling Guidelines

Data Handling Guidelines

These guidelines are to provide guidance to data custodians as to how they may protect data classified under the headings defined in the Data Classification policy. (See Appendix A for Data classification.) These guidelines are considered best practice for the protection of that data.

Classification/ Activity	**DCU Highly Restricted**	**DCU Restricted**	**DCU Controlled**
Access Control	Available only to those who have an absolute requirement for access. This requirement must be submitted in writing and authorized by the data custodian. Access should be reviewed on a regular basis. Where access is granted to a third party, a non-disclosure agreement should be in place.	Available to authorized users only. Access should be reviewed on a regular basis. Where access is granted to a third party, a non-disclosure agreement should be in place.	Available to all DCU employees and others as required.
Backup	Data should be highly protected. Backups should be taken on a nightly basis, subject to data change rate. Backups should be held in a secure fire-proof-location removed from the data source. This data is a candidate for online mirroring to a remote location.	Data should be protected by backups and held in a secure location away from the source data.	Data should be protected by backup.

Classification/ Activity	DCU Highly Restricted	DCU Restricted	DCU Controlled
Labelling	Irrespective of the data classification labels should be used to convey the importance of the data where appropriate, e.g. Confidential or Strictly Confidential.		
Physical Transfer (paper)	For classifications of data due care should be taken in respect of the transfer of information in physical form.		
Electronic Storage	Must be stored in systems accessible only to those covered under access above. Servers which hold this data must be housed in a secure datacenter environment. Storage of this data outside of the source system, for example on a laptop or memory stick; must be approved by the data custodian. Where data is held outside the source system it must be encrypted. Where a mobile device is used to access/store DCU sensitive data or email, appropriate security settings must be configured. USB devices must not be used for	Must be stored in systems accessible only to those covered under access above. Where data is held outside the source system it must be encrypted.	Must be stored in systems accessible to those covered under access above.

	the storage of sensitive personal data. Encryption software must be installed on all DCU owned laptops.		
Electronic Transfer – Internal to DCU	Data transfers need to be encrypted. USB devices must not be used for the transfer of sensitive personal data.	Where possible data transfers should be encrypted. Transmission over a wireless network needs to be encrypted.	Encryption should be considered where appropriate
Electronic Transfer – External to DCU	Data transfers need to be encrypted. May not be emailed unless encrypted. USB devices must not be used for the transfer of sensitive personal data.	Where possible data transfers should be encrypted. May not be emailed unless encrypted.	Encryption should be considered where appropriate.
Disposal	Physical copies of data should be shredded. Storage media, including hard drives which have ever held such data should be disposed of in a secure manner. Please consult ISS for further information.	Physical copies of data should be shredded. Storage media, including hard drives which have ever held such data should be disposed of in a secure manner. Please consult ISS for further information.	Systems handling data may be disposed of in a normal fashion.

Classification/ Activity	DCU Highly Restricted	DCU Restricted	DCU Controlled
System Controls	Information may only be processed on approved DCU systems, which are managed by a designated systems manager.	Information may only be processed on approved DCU systems, which are managed by a designated systems manager.	Information should be processed on the basis of basic best practice.
System Availability	Where the data availability requirement is high, consideration should be given to hosting this data on a resilient infrastructure which would protect against outages.	Information should be subject to the appropriate industry standards which ensure the availability of the information when and where required.	Information should be subject to the appropriate industry standards which ensure the availability of the information.

Appendix A – Data Classification

Data Classification	**DCU Controlled** With this classification protection of information is at the discretion of the custodian and there is a low risk of embarrassment or reputational harm to DCU. *Examples*: Meeting minutes; unit working & draft documents	**DCU Restricted** DCU has a legal, regulatory or contractual obligation to protect the information with this classification. Disclosure or loss of availability or integrity could cause harm to the reputation of DCU, or may have short term financial impact on the university. *Examples*: Student or employee records; grades; employee performance reviews; personally identifiable information.	**DCU Highly Restricted** Protection of information is required by law or regulatory instrument. The information within this classification is subject to strictly limited distribution within and outside the University. Disclosure would cause exceptional or long term damage to the reputation of DCU, or risk to those whose information is disclosed, or may have serious or long term negative financial impact on the University. *Examples*: PPS numbers; Physical or mental health record relating to individuals; Critical research data.