TU Dublin Guidelines for Data Encryption

Purpose

The purpose is to provide guidance on the encryption of (strictly) confidential and/or personal information contained, processed or transmitted within hardware and software resources that are owned and/or operated by the University.

Scope

This applies to all University staff and students as well as any external parties (e.g. contractors, etc.) with access to information hardware and software resources. It covers (strictly) confidential/personal data at rest (data stored), data in transit (transmission of information), and also encryption key standards and management. It also addresses all (remote or on site) connections made to University domains (e.g. WiFi, LAN etc.), and all connections made to external sites through the University's network.

Situations Requiring Encryption

Encryption is necessary in order to protect (strictly) confidential/personal data pertaining to employees, students and other affiliates of the University and is required in the following situations (among others):

- Disk encryption for laptop and desktop computers.
- Password encryption/hashing.
- Backup data where the backup media is sent outside of an University facility or a facility managed on behalf of the University.
- Remote access and VPN communication channels.
- Mobile computing equipment storage media and backups.
- Data communications for externally facing applications transferring (strictly) confidential and/or personal data (as defined under GDPR).
- Web services communication/interactions transferring (strictly) confidential and/or personal data (as defined under GDPR) beyond the University's data centre.

Data at Rest

Data at rest is data that is saved in persistent storage like disks or tape. Data at rest can reside in the file system or in the data tier as individual data elements. Encrypting data at rest protects sensitive data and meets regulatory compliance requirements.

Depending on its data classification, data at rest may need to be encrypted so it is not readable by any user or application without a valid key.

- For internal data: Encryption not required.
- For confidential data: Encryption required anywhere

- For strictly confidential data: Encryption required anywhere.

Strong key management is required for encrypted data at rest to reduce the risk of unauthorised access to the data. How this policy applies to each device owned and/or operated by the University is summarised below:

1) <u>Servers</u>

(Strictly) confidential data stored on shared network servers which are situated in insecure locations (e.g. remote print servers) must be protected by the use of strict access controls and encryption software.

2) <u>Laptops & Desktop Computers</u>

(Strictly) confidential data at rest on computers owned by the University and located within controlled spaces and networks should be protected by encryption with strict access controls that authenticate the identity of those individuals accessing the specific system or data.

Encryption software should be installed in the following:

A. Any computer owed and/or operated by the University that is located in an external (third party) facility.
B. Any computer owed and/or operated by the University that is located in a public area (e.g. at a reception desk).
C. Any computer owed and/or operated by the University that is located in the home of an University employee.
D. Any computer owed and/or operated by the University that permanently stores (strictly) confidential/personal information or hosts information systems that process such data on the local hard drive, rather than on a secure server.
E. The method of encryption required for the University's computer devices is whole disk encryption.

3) <u>Tablets, Mobile Phones and other Smart Devices</u>

(Strictly) confidential data should not be stored on these portable devices, as loss or theft of these devices can result in unauthorised data exposure and thus constitute a data breach. If (strictly) confidential information must be stored on such devices, whole disk encryption reduces the risk of unauthorised data access should the theft or loss of the device occur.

All portable devices must have up to date antivirus software and password protection enabled, in addition to data encryption.

All users should obtain permission from the Data Protection Officer prior to storing (strictly) confidential information on portable devices, and under <u>no</u> circumstances should these devices be used for the long term storage of such information.

Portable or removable media that contain (strictly) confidential data must be in the possession of the authorised user at all times (e.g., must not be checked as luggage). Users of portable computing

devices containing (strictly) confidential data must acknowledge how they will ensure that data are encrypted and how encrypted data will be accessible by the owner in the event that an encryption key becomes lost or forgotten. This can be done by:

- Maintaining a copy of each encryption key in usage on a secure server managed by the University, including procedures specified by the DPO.
- Using encryption that allows an authorised system administrator access to the data in the event that an encryption key is forgotten.

4) Removable Storage Devices

(Strictly) confidential data should not be stored on any removable storage device

Data Transmission

All (strictly) confidential or restricted information transmitted through email to an email address outside of the University's domain must be encrypted. The transfer of such information must be authorised by the Head of School/Function and/or the DPO. The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

Where (strictly) confidential and restricted information is transmitted through a public network (for example the internet) to an external third party the information must be encrypted first or sent via a secure channels (for example: HEANET file sender). The transfer must be authorised by the Head of School/Function and/or the DPO. The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

If a secure server is used to enable the encrypted transfer of documents and data over the Internet using file transfer programs, each authorized user must have a logon ID and password with a designated directory. All accounts and keys must be managed from within network. All transactions and transfers must be logged, and reviewed for prohibited activity.

Encryption Key Management

Effective key management is the crucial element for ensuring the security of any encryption system. Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.

The individual with responsibility for encryption key management (e.g. Head of IT, etc.) will verify backup storage for Key passwords, files, and related backup configuration data to avoid single point of failure and ensure access to encrypted data.

Separation of duties and two person control prevent the generation of a new encryption key by a single individual. Regular (e.g. quarterly) reviews will be conducted to verify the identity of all subjects responsible for key management functions and the generation of new encryption keys. Training should be provided to all relevant personnel on key management requirements and procedures.

Keys must be randomly chosen from the entire key space, using hardware-based randomization. Key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key, e.g., a key-encrypting-key is used to encrypt other keys, securing them from disclosure. The following points are also addressed by encryption key management policy:

- Encryption keys that support a production environment must be bound to the University.
- All encryption keys and key management procedures must have an identified owner to ensure accountability to an individual identity within the University.
- Cryptographic modules that are used for storing keys must be backed up using approved encryption strength technology (e.g. accredited to FIPS 140-2 Level 2).
- Private keys must be kept confidential.
- Keys in transit and storage must be encrypted.
- Keys must be destroyed at the end of their crypto period.
- Key-generating equipment is kept physically and logically secure from construction through receipt, installation, operation, and removal from service.