Dublin City University

Removable Media Security

Introduction

As a general rule, you should not store sensitive information on a USB or other portable storage device. If you do need to store sensitive data on a storage device, encrypt the device. See ISS encryption service FAQ's for more information.

In the event that your portable device is lost or stolen, encryption will prevent an unauthorized third party from accessing your device's contents. If someone tries to break into your device to retrieve files, they will not be able to access any files without your password.

Risk of Infection

The integrity of data on your removable media, such as memory sticks or external hard drives, is potentially at risk every time you plug it to a computer if that computer is infected. Conversely, if your removable media is infected, then you run the risk of infecting any unprotected computers that you plug your removable media into, thus putting other users of that computer at risk.

To reduce the risk of infection:

1. Before you plug an external device to PC or laptop run the virus checker and anti-spyware software. If the computer is infected you will need to disinfect the computer. If you suspect that your computer has been compromised in any way consult your local IT staff or the ISS Help Desk immediately.
2. You must also ensure that the computer is not at risk from infected files on your external storage device. Only plug your external devices into protected, trusted computers and regularly run your virus checker and anti-spyware software on your external devices.

Physical safety of external devices and the data on them

To increase the security of your removable devices**:**

1. Ensure that your external storage media are safe from theft, loss or destruction
2. Apart from the storage media itself, make sure that data contained on them are also safe from theft. If your device contains DCU Restricted or DCU Highly Restricted data or data classed as sensitive under the Data Protection Act, you must encrypt these devices so that the data on them cannot be accessed without the encryption key. ISS encryption service FAQ's provides more information on DCU's encryption service.

Secure disposal of removable storage media

All drives /storage media that has contained DCU Restricted or DCU Highly Restricted Data must be delivered to ISS for secure disposal. Please contact the ISS ServiceDesk for further information.