Dublin City University

Mobile Computing Policy

Contents

Purpose 1
Scope 1
General Information 1
Security Requirements..... 2
Document Change Management..... 3

Purpose

The purpose of this policy is to ensure that effective measures are in place to protect data in respect of the use of mobile computing, communication and storage devices. Protection should be in place to avoid the unauthorised access to or disclosure of DCU sensitive data stored and processed by these devices.

Scope

This policy applies to all DCU employees and students using mobile computing devices (laptops, PDAs etc.), mobile communication devices (mobile phones, smart phones etc.) and mobile storage devices (USB memory sticks, CD/DVD's etc.) to access DCU resources in public places, meeting rooms, and other unprotected areas both within and outside the Dublin City University campus. Where it is necessary to store sensitive data on these devices, users are required to observe this policy to assure that all possible steps have been taken to keep the university's sensitive data secure. Note that this policy applies equally to information stored on or accessed via home PCs.

Mobile Computing devices used by contractors, or third parties, to access the DCU network, applications, and/or data are subject to the appropriate ICT Policies and guidelines, e.g. Network Connectivity Policy, Remote Access Policy, ICT Compliance Policy, Data Classification Policy and Data Handling Guidelines.

Templates covering the provision of goods and/or services by Third Parties to DCU are available from the Procurement Office, Finance Department, DCU.

General Information

1. Mobile computing, communication and storage devices have become popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognized and addressed to protect both the physical devices and the information they contain. Special security issues that relate to mobile devices include the following:
    a. Any malware (viruses, worms, Trojans) that infect the device can bypass the university's security and spread

rapidly to other devices once connected back to the network;

b. If data stored on a mobile device is not backed up by the user it could be completely lost if the device is stolen or fails;
c. Any sensitive data stored on a mobile device would be compromised should it be stolen or lost.

2. Users should be familiar and comply with the following related documents;
   a. Remote Access Policy
   b. Network Connectivity Policy
   c. *Data Handling Guidelines*
   d. Data Protection Guidelines

Security Requirements

1. The following security controls, when available, must be activated on all devices to help protect against theft of sensitive DCU information contained on the device:
   a. Encryption software must be installed on all DCU owned laptops. USB devices must not be used to store/transfer sensitive personal data.
   b. All mobile devices must have a password protected keyboard/screen lock that is automatically activated by a period of inactivity. The inactivity time interval should be no more than 15 minutes.
2. When not at your desk for an extended period of time your device must be physically secured (i.e., locked in a desk drawer or filing cabinet, locked in an office, or taken with you).
3. When travelling, the following is recommended practice where possible;
   - Keep devices in your possession at all times.
   - Do not put devices in checked baggage, and be alert to the possibility of theft when going through security checkpoints at airports.
4. When using a laptop, do not process personal or sensitive data in public places e.g. on public transport.
5. Passwords for access to DCU systems should never be stored on mobile devices where they may be stolen or permit unauthorized access to information assets
6. If your mobile device is stolen or lost, you must report the loss immediately to DCU's Data Protection Officer.

Document Change Management

Dublin City University believes that it is important to keep this policy current in order to ensure that it addresses security issues accurately and is up-to-date with evolving business issues and technologies. This policy is a living document that will be reviewed annually and/or updated as needed.

The Director of Information Systems and Services will draft necessary changes and have them reviewed and approved by the Executive Group of DCU as appropriate. The Director of ISS and the members of the ICT Security Implementation Group will communicate changes to the University communities. Anyone in the University can determine the need for a modification to the existing policy. Recommendations for changes to this policy should be communicated to the Director of ISS.