GUIDANCE ON PASSWORD CHOICE AND STORAGE

Introduction

Within the University IT regulations it states that:

> *"Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or **passwords allocated for their use**. Users must not use access codes that belong to someone else."*

Passwords are the standard method for access to systems, and as such **must** be protected. While great efforts are taken to integrate University systems together so that a standard username and password can be used for most systems, it is recognised that staff may need access to a system as part of their role that cannot be integrated or are provided by 3rd parties, and it may be difficult for staff to memorise multiple passwords.

This document provides guidance on choice and storage of passwords.

General advice on password choice

Picking a good password is important, however in accordance with University Password Policy all passwords must be over 8 characters, contain a mixture of upper case, lower case and symbols, must not be re-used, and should not be a word listed in a dictionary.

More complex random passwords can be generated, and tools such as KeePass or LastPass include inbuilt password generation.

The same username/password combination as used for University systems **must not** be used for 3rd party systems, as a compromise of this system would then directly compromise the University infrastructure.

A good guide on selecting passwords is available online at
http://www.bu.edu/infosec/howtos/how-to-choose-a-password/

Guidance on password storage

If it is felt necessary to store passwords then they **must never be**:

- stored in unencrypted files
- written down
- left in unsecured locations

It is recommended that if passwords have to be stored electronically they are stored on secure file shares or University sites with access control enabled to limit access to authorised

University staff. Storing on a University provided service provides resilience in case of deletion or corruption of the password file. Permissions and access to the files should be checked to ensure that it is accessible to the minimum number of people who need to have access.

Word 2007 or higher versions in the "DOCX" format which are also password protected provide the minimum level of security required. Note the old Word 2003 ".DOC" format is not secure and must never be used for password storage.

Password Managers such as KeePass or Last Pass provide secure storage of passwords, with inbuilt password generation. KeePass files can be stored on a secure file share for resilience.

KeePass is free open source utility available online at http://keepass.info/

LastPass is a web based service available free to individuals online at https://lastpass.com/