Password Policy

1.0 Overview

Information stored on the computer desktop and the LAN (local area network) forms a part of the university's valuable assets. Strong passwords promote a secure computing environment consistent with Section V Part 2 of the Electronic Communications Policy. To counter the forces of social engineering (this happens when an attacker tricks users into divulging passwords.) and brute force (these are attempts to gain unauthorised access to systems by trying every combination of letters and numbers until a match is found that allow access) methods of attack, we must be diligent in guarding access to our resources from internal and external threats by adopting strong passwords.

Passwords are the primary authentication method for the university's IT resources and are currently the basic authentication method employed. Passwords ensure that only authorised individuals have access to specific computer systems and establish accountability for all changes made to system resources. Badly chosen passwords endanger the information that they are supposed to protect.

The university needs to institute a robust password policy if it is to move towards a single- sign-on environment. With a single-sign-on system, a user will be required to authenticate once to gain access to all network resources.

2.0 Scope

This policy applies to all permanent faculties, staff and students and temporary faculty staff and students, associated students and staff affiliated with the University of Westminster, and any external contractors who are given computer accounts to access information systems owned by or operated by The University of Westminster.

3.0 Best practices.

- Passwords should not be written down, emailed or spoken.
- Passwords must be kept confidential and not shared with colleagues. This does not apply to generic departmental passwords, where a group manages the password.
- Your username or variations of the username should not be embedded in your password.
- Passwords must not be blank.
- Passwords should not be typed or saved in electronic documents
- Computer generated passwords must be changed following initial successful login.
- Passwords must not be based on personal information (e.g. names of families, pets, name of your street, car registration numbers, telephone numbers)
- Passwords must not be revealed to your line manager.
- Passwords must not be revealed to anyone over the phone even if the recipient is a member of the Campus computer Team or ISLS.
- Passwords used within the university must not be used for external Internet accounts or online service providers.
- Passwords must not include words from a dictionary in any language.
- Passwords must not be included in any automated login process.

- New passwords must not bear any relation to the old. For instance, if the old password is April, the new password must not be April1 or 1lirpa or any variation of April.
- Once the passwords have been changed, the new password must be kept for 8 days before the user can be allowed to change it again.
- Passwords must be unique from previous passwords. The previous passwords should not be re-used.

4.0 Password Composition

4.1 Desktop/client operating systems:
Passwords must meet the following criteria:

- Passwords must be at least six characters long.
- Passwords must be composed of alphanumeric characters (alphabets – A..Z, a...z and numbers – base 10 digits – 0..9).
- Passwords should include non-alphanumeric or special characters (e.g. !; £; $;); (; %; &; *; #; @; ?; {; }; [;]; =; +; >; <; “;).
- Passwords must be strong.

Here are some methods for making strong passwords:

- You can choose one or two lines from a poem or song and use the first letter of each word. For example ‘**A**lways **l**ook **o**n **t**he **b**righ**t** **s**ide **o**f **l**ife becomes alotbsol

- Passwords are case sensitive: using the above example, the passwords **alotbso**l**, AlotbsoL** and **aLotBsol** are different and the security of passwords can be increased if mixed case passwords are used.

- One strategy for creating strong passwords is to replace letters with numbers or characters. For example A**lo**tbs**ol** becomes A**10**tbs**01** where the letter **“l”** has been replaced with the digit “1” and the letter **“o”** has been replaced with the digit ‘**0**’**.**
- Choose a minimum of two short unrelated words and concatenate them together with special symbols or numbers. For example, **awn, crat, it** are three unrelated words which become **awn+crat=it?** when the words are joined together.

5.0 Changing your password
Passwords must be changed under any one of the following circumstances:

- At least every three months
- Immediately, if a password has been compromised or after you suspect that a password has been compromised.
- Passwords must be changed on direction from Campus Helpdesk or ISLS staff.

Note: You should not change your password last thing on Friday or just before you go on holiday as you may forget it when you need to use it.

6.0 System based Password Requirements
Privileged and administrative passwords must be subject to stringent composition and frequency of change. Privilege passwords include passwords for routers, switches, hubs, firewalls, network operating systems and any other IS resource.

6.1 Good practice/handling

- All Passwords must be documented in the password book and kept in the safe at all times. Only authorised personnel must access the safe.
- Passwords must be unique for every server system.
- A number of shared local administrative passwords may be used on machines for specific departments and computer labs.
- Passwords must be at least eight characters long but preferably longer.
- The root/super user password must never be used unencrypted across the network to avoid eavesdropping. Wherever possible you must **su** to root using SSH or similar technology or use sudo.
- Passwords must be retired after three months.
- Once the passwords have been changed, the new password must be kept for 8 days before the user can be allowed to change it again.
- Service accounts must not rely on admin accounts/passwords.
- Accounts created for external contractors should be given restrictive rights to carry out their functions and the accounts should be disabled immediately following the completion of the appointed task.
- Administrator/privielege passwords must not be disclosed to external contractors.
- Default passwords that come with computer systems or services must be changed during installation or immediately after installation.
- Passwords must be unique from all previous passwords. The last ten passwords must no be re-used.
- All systems must wherever possible be set up to prompt the user to change passwords in seven days.
- Critical systems must implement account lockout policies and be set up to disconnect idle sessions after a period of inactivity of thirty minutes.
- Systems must be configured to enforce password changes.
- The SNMP community strings must be changed from the standards defaults and should be different from the password used to interactively log in.
- Privileged passwords should not be communicated via telephone fax or email.

7.0 Password changes
All passwords must be changed via the web interface http://password.wmin.ac.uk.

8.0 Enforcement
Failure to observe these regulations will be regarded as an infringement of the Electronic Communications Policy and may be subject to disciplinary action.

9.0 Responsible Officer

The IS Director and the Network Security Officer will be responsible for the maintenance and review of this policy.

Version 1.4 – June 2003