Information Security Management

UNIVERSITY OF LEEDS

Password Usage and Management Policy

Version 1.2
16 December 2008

Owner:	Kevin Darley, IT Security Co-ordinator, Information Systems Services, University of Leeds
Source Location:	M:\Policy\Issued\Password Usage and Management Policy.doc
Document Reference:	
Other Documents Referenced:	
Related Documents:	Information Security Policy, Password Usage and Management Policy, Systems Security and Network Access and Management Policy, Mobile and Remote Working Policy, Software Usage and Control Policy and Archiving Policy
Acknowledgements:	

Document Control

This document is subject to change control and any amendments will be recorded below.

Change History

Version	Date	Circulation	Changes
1.0	25/10/05	http://campus.leeds.ac.uk/isms	First formal issue
1.1	08/08/07	http://campus.leeds.ac.uk/isms	General review
1.2	16/12/08	http://campus.leeds.ac.uk/isms	Changes to reflect new policy for students.

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available at http://campus.leeds.ac.uk/isms. Those to whom this Policy applies are responsible for familiarising themselves periodically with the latest version and for complying with Policy requirements at all times.

Contents

1. Introduction 4
1.1. Background 4
1.2. Applicability 4
1.3. Scope 5
2. Password Usage and Management 5
2.1. Purpose and Overview of Policy 5
2.2. Secrecy & Divulgence of Passwords 5
2.3. Password Storage and Configuration of Microsoft Windows Systems 5
2.4. Password Complexity and Choice 6
2.5. Password Aging and Forced Password Change 6
2.6. Unforced Password Change 6
2.7. Systems-Level (Administrator and Super-User) Passwords 7
2.8. Shared Password 8
2.9. Compliance Monitoring 8
2.10. Password Resets 8
2.11. Help and Assistance 9
3. Annex ..... Error! Bookmark not defined.
3.1. Selecting a Strong Password 9
3.2. Protecting Your Passwords 10

1. Introduction

1.1. Background

Although technical and procedural controls are applied throughout the University's IT/IS infrastructure to protect facilities and data from unauthorised access, provision has to be made for legitimate users to access data relevant to their normal University activities where and when they need it. This is controlled through the issuance and management of user accounts, which are designed to ensure that users are able to gain access to data and services relevant to their needs.

Before a user can access the systems and data associated with their user account(s), a process of authentication is carried out which validates the access that a user is requesting, against the permissions that individual has been granted. Key to this process is the input of the user's user-id and password, which effectively presents their 'electronic identity'.

In order to provide accountability and to prevent misuse and abuse of their 'electronic identity' by others, it is crucial that passwords are both strong and managed diligently. The importance of this requirement cannot be overstated as the University moves towards 'Simplified Sign-On' (SSO) where the authentication process of user names and passwords will provide access to multiple systems and data to which account holders have been granted privileges.

This document which forms the University's *Password Usage and Management Policy*, in support of the University's *Information Security Policy*, defines the password controls that are designed to protect users, systems and data. The University's *Information Security Policy* and a full list of Supporting Policies within the Information Security Management System (ISMS) framework can be found at http://campus.leeds.ac.uk/isms.

1.2. Applicability

This policy applies to the following:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of the University;
- Registered students of the University;
- Contractors and consultants working for or on behalf of the University;
- All other individuals and groups who have been granted access to the University's IT/IS and network facilities, including visitors.

It is the personal responsibility of each person to whom this Policy applies to adhere fully with its requirements. However, Deans and Heads of Schools/Services[1] are responsible for implementing this Policy within their respective faculty/school/department and for overseeing compliance by those under their direction or supervision.

[1] Also generically infers Heads of Centres & Institutes throughout.

1.3. Scope

This Policy concerns all[2] computer systems operated by the University, regardless of location, where responsibility for user management and control resides with members of the University.

Systems that are hosted at the University but which are controlled or operated by third parties who are not under the University's jurisdiction are not subject to this Policy.

2. Password Usage and Management

2.1. Purpose and Overview of Policy

The purpose of this policy is to stipulate the need for users to choose 'strong passwords', and define the management controls required for users to protect them.

Passwords are an important component for the protection data and information systems within the University. They are the front line of defence for user accounts and they will become increasingly important as the University moves towards 'simplified sign-on', where a single log-on will provide access to more applications and data resources.

Strong passwords are important because weak passwords are more easily compromised through 'social engineering' or may be guessable by those who know the user. Furthermore, password cracking software tools could be used to scan systems at high speed looking for passwords comprising of plain words or those where numbers have been used to simply replace characters (e.g. f00tba11).

All users of University computing facilities are responsible for taking appropriate steps, as outlined below, to select and secure their passwords. Guidelines for choosing strong passwords can be found at the Annex.

2.2. Secrecy & Divulgence of Passwords

Individuals are personally responsible for maintaining the secrecy of their passwords and for controlling access to their user accounts through password security.

Passwords are not to be divulged by users to anyone except a computer support engineers who are in their presence and only when there is a fault with user's computer or the user's network access. In such circumstances the password must be changed as soon as the engineer has finished (see 2.6.4). Passwords must never be divulged over the telephone or in an e-mail.

2.3. Password Storage and Configuration of Microsoft Windows Systems

It is the responsibility of systems administrators to ensure that only hashed/encoded forms of password are stored in their respective systems.

Where practicable, Microsoft Windows systems should always be configured so that they don't store the LM hash values of user's passwords.

[2] Except any systems which authenticate users without using passwords.

2.4. Password Complexity and Choice

2.4.1 Password Complexity

The University will not necessarily configure its systems to enforce password complexity but users are required to choose strong passwords (see 2.4.2).

2.4.2 Password Choice

Users are required to choose sensible strong passwords at all times in order to protect their 'electronic identity', prevent unauthorised access to systems and preserve the availability and integrity of data.

Guidelines for choosing strong passwords can be found at the Annex. All passwords used have to be unique i.e. you are not allowed to recycle passwords.

2.5. Password Aging and Forced Password Change

2.5.1 Forced Password Change

Administrators who operate their own systems (independent of Active Directory) are required to implement a process to force-change the password of newly created accounts at first log-on, where this is technically possible.

2.5.2 Password Aging

The University will not implement password aging, except in respect of those passwords that provide access to certain financial and other sensitive applications. However, where password aging is enforced for financial and sensitive applications, system-forced changes will occur at least every 45 days.

2.6. Unforced Password Change

2.6.1 Users at Initial Logon

Users of systems that cannot be configured to force-change their initial default passwords at first logon are required to change them themselves at the first logon.

2.6.2 Default Passwords

System administrators and computer support staff who configure new systems and set up services are to ensure that all password settings are changed from their default settings before moving platforms into production.

This is particularly important in the case of databases (such as Oracle) that use standard (well known) default passwords. These must not be used and default passwords must be changed as soon as possible after a new system is acquired, or after any database or operating system upgrades that re-instate default accounts and passwords.

Peripherals with embedded software, such as printers, plotters and webcams, often have default or null passwords which must be reset.

2.6.3 System-Level Passwords

All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed on at least a quarterly basis. However, where it is where practical changes should be implemented monthly.

2.6.4 User Passwords

It is recommended that user passwords are changed at least every six months. They must be changed immediately on any occasion that a user believes that someone else may be aware of their password and on all occasions when a malpractice incident is discovered or suspected.

2.6.5 Temporary Accounts Passwords

Each custodian of temporary accounts must change the password of each temporary account back to its master setting on each occasion that a temporary user leaves or no longer requires access to the account in question. Custodians are also responsible for ensuring that a new and unique password is applied to each temporary account on each occasion that they are issued/reissued to a new user.

Temporary accounts that are used purely for training purposes are exempt from this requirement.

2.7. Systems-Level (Administrator and Super-User) Passwords

Staff may only have access to system-level passwords on a need to know operational basis, not because they may possibility need them at some time.

Shared administrator and super-user (global) passwords are not to be used on production systems except where passwords are hard-coded into applications. It is strongly recommended that this rule is also applied to development and research systems.

On Windows systems passwords for privileged accounts must be 15 characters or more[3].

Administrators and IT support staff are to be allocated secondary accounts which have the appropriate rights and privileges to enable them to support the systems and services for which they have a responsibility. This should be done in all cases where hard-coded passwords are not required.

UNIX users are to use their own user accounts to SU to Root.

2.7.1 Hard-Coded and Service Account Passwords

Hard coded and service account passwords must never be used to log onto servers.

Where practical, hard-coded and service account passwords are to be changed on a quarterly basis and the change is to be performed in a synchronized manner to avoid operational problems. Where password changes are due on a Friday they are to be deferred until the next working day.

[3] Windows generates and stores user account passwords in two different password representations; LM hash and NT hash. The LM hash is relatively weak compared to the NT hash, and it is therefore prone to fast brute force attack. If a password contains 15 characters or more, Windows will not generate and store the weaker LM hash version.

2.8. Shared Password

Passwords are not to be shared by users, except in the case of administrators and IT support staff who are responsible for the maintenance of systems and services that utilise hard-coded passwords (see 2.7.1).

Where there is a need for several users to have access to common data and mail boxes, such as those working collaboratively, access must be controlled in accordance with the *Access Control and Account Management Policy*.

2.9. Compliance Monitoring

Password cracking tools may be operated by ISS on a random or periodic basis in a bid to identify weak passwords. Before doing this authority must first be obtained from the IT Security Co-ordinator.

2.10. Password Resets

2.10.1 Staff Passwords

The identity and association of a person with a particular account must be verified by administrators prior to resetting their password.

Passwords must not generally be re-armed on the basis of an e-mail request or telephone call from the user regardless of the level of authority that the requester may have.

Passwords must generally only be reset when the person requesting a re-arm is present and has been properly identified and verified against held documentation as being the account holder. However, ISS Username Administration staff or system administrators, as applicable, may re-arm the passwords of staff who are not based on campus A process is to be established so that such requests can be made by telephone by using agreed shared personal information that the account holders and ISS Username Administration staff / system administrators are party to.

Only recognised User-Representatives may request the password re-arm of a third party ISS user account, where the user has forgotten their password and is unable to attend the Help Desk. Passwords must not be re-armed on the basis of any other third party request, regardless of the status of the individual making the request.

However, ISS staff and User-Representatives may request a re-arm of a user's password in order to identify or fix a fault, and User-Representatives can request a user's password to be re-set when it is necessary to migrate services in the user's absence. In both cases, the user is to be informed of the new password at the first opportunity by the person who has requested the re-arm, and is to change this at the next logon.

User-Representatives are to maintain a log of all password re-arms and account suspensions that they request.

2.10.2 Student Passwords

A password self-service re-set facility ('Quest') has been provided for students, the use of which is mandatory. All students are required to register with the service at https://passwordreset.leeds.ac.uk and provide answers to security questions. To re-set their

password, students will need to answer a selection of the questions for which they have provided answers for. All students' passwords must:

- comprise a minimum of eight characters;
- contain at least one number;
- not have been used before.

Initially, this policy will only be enforced when students change their password. However, in 2009 all students will have to change their password to comply with the new policy. Details of this requirement will be communicated in advance.

2.11. Help and Assistance

Students who forget their password may use the 'mypasswd' facility in order to establish the details. However, this will only be of use if they have not previously changed their initial password (Ref. 2.6) as the details of the new password will not be available from the mypasswd facility.

Any questions regarding the use and management of passwords should be directed to the ISS Help Desk which operates Monday to Friday from 08:00 hours to 18:00 hours (summer) and 08:00 hours to 21:00 hours (winter). The Help Desk is also open on Saturdays from 12:00 hours to 17:00 hours during term time.

3. Annex

3.1. Selecting a Strong Password

1. When you choose a password you should make it personally memorable but difficult for others to guess:

- Make sure that your password comprises at least 8 characters but do not use special characters as they may not be recognised by some systems;
- Make sure that your password comprises at least 8 characters [4];
- Choose one that is easily remembered;
- Never write your password down;
- Immediately change your password if you think that it has been revealed to anyone else or compromised;
- Never use your user name in any form as your password;
- Never use your surname or given name in any form;
- Don't use any information about you that is easily obtainable, such as your car registration number, your birthday, your child or pets name, your favourite holiday destination or your favourite sports team or hobby;
- Don't use word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.;

[4] Some systems only use the first 8 characters of a password so numerics should be use within the first 8 characters.

- Avoid the use of an ordinary word preceded or followed by a digit (e.g., secret1, 1secret);
- Don't change your password by simply adding a number every time you have to change it;
- Don't reuse or recycle your password;
- Don't share your passwords with anyone, including administrative assistants or secretaries;
- Never use the same password for both your university and private computer accounts, such as on-line banking, Facebook etc.;
- Don't use the 'Remember Password' feature of applications.

If someone demands a password, refer them to this Policy or have them contact the IT Security Co-ordinator.

2. In addition, make sure that your password is:

- Private - it is used and known by you only – you wouldn't like it if your identity was stolen, so why give it away?
- Not shared, even with your secretary – if you have a secretary who has a need to access your data, this can be facilitated through file permissions for both Exchange and File Store;
- Secret - it does not appear in clear text in any file or program in any medium.

3. Use one of the following methods to create a memorable but strong password:

- Use the first letter of each word in a memorable phrase, saying, nursery rhyme or song title. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. Please do not use this example.
- Substitute one or more letters with a numeric character (e.g. I = 1, A = 4, S = 5, L = 7 or O = 0);
- Take two words and splice them together with one or more non-alphanumeric characters, or;
- Take an ordinary word or phrase and change, delete or add characters so that it becomes nonsensical.

3.2. Protecting Your Passwords

In order to ensure that both University data and your information are protected, system users are held responsible for safeguarding passwords and access identities. Passwords and identities must not be shared. System users are responsible for all use of information systems and technology and for any information stored or communicated using their identity or password.

All individuals' usernames issued at the University are unique and are not reused. Although usernames are not secret, they should be treated as personal. Details are not published and they should not be divulged to others.

Passwords on the other hand are secret and you are responsible for protecting your own. If you are the only one who knows your password your information is and the systems that you access are safe.

Remember that a computer that is left unattended and logged in gives anyone access to information accessible to the authorised user. If a computer is left unattended, it should be shut down or locked through the use of a password access 'hot-key' or password protected screen saver.