Standard

Passwords

Information Security Manager

For latest version and information about, see lse.ac.uk/policies and search by title.

Document control

Distribution list

Name	Title	Department
Adrian Ellison	Assistant Director, Infrastructure Services	IT Services
Amber Miro	Assistant Director, User Services	IT Services
Andy Coulthard	Assistant Director, Management Information Systems	IT Services
Puneet Singh	Systems Manager	Technical Infrastructure Group, IT Services
Malcolm Barker	Network Manager	Technical Infrastructure Group, IT Services
Stephan Freeman	Information Security Manager	Technical Infrastructure Group, IT Services
James Hargrave	User Support Manager	User Support, IT Services
Tim Green	IT Manager	Library
Nic Warner	Computer Manager	STICERD

External document references

Title	Version	Date	Author

Version history

Date	Version	Comments
15/04/2011	1.1	Incorporated comments from AE
19/10/2011	1.3	Changed password-change interval to “annual” to reflect discussions at various committees.

Review control

Reviewer	Section	Comments	Actions agreed
AE	All	Tracked changes	

Table of contents

Introduction

Purpose

This document sets out the minimum length, complexity and rotation for user passwords in LSE systems, and specifies the parameters that can be set within Active Directory to improve security further.

Scope

These password standards apply to *all* types of user specified in the document **ISM-PY-016 User Accounts** and across all systems that support the controls outlined in this document.

Background

LSE has traditionally had weak password controls, with the oldest password as at December 2010 being 16 years-old. Given the way in which the old Windows NT 4 domains were amalgamated into the Active Directory, users were not required to change their passwords and, therefore, adhere to the most-recent round of minimum password requirements, which were set at five characters.
This means that several hundred users still have three character passwords.
Passwords are the only method of authentication at LSE and are, therefore, critical to the protection of data across the School.
The measures outlined are designed to reduce the opportunity for misuse of a compromised password and increase the length of time an attacker will need to "crack" any given password.

Assumptions

It is assumed that systems can apply the controls outlined in this document. For systems where this is not possible then the Information Security Manager should be contacted.
The reader has a good understanding of the concepts and terminology used throughout this document.

Conventions

A number of different styles of text and page layout are used within this document. This section describes the use of these styles together with examples.

Font styles

Bold is used to emphasise important information.

Italic is used for file and directory names, URLs and registry key names. Italic is also used to indicate a filename or comments within a code section. Italic is also used for the first reference to a vendor or product where doing so improves clarity.

`Constant width` is used to indicate sections of code and program names.

`Constant width with italic` is used to indicate parts of code to be replaced depending on certain conditions.

`Constant width with bold` is used to indicate text typed by the user in code sections.

Bullets

Bullets appear indented in relation to the paragraph indentation with a nested bullet available in a different style:

- Bullet
    - Nested bullet

Notes, warnings, tips and suggestions

Notes, warnings, tips and suggestions are

These boxes hold important details relevant to the surrounding text

Tables

Tables appear as follows:

Header Row (Repeated on each page if the table splits across a page)
Data Row

Responsibilities

It is the responsibility of all staff in IT Services and other areas authorised to procure IT systems responsible for assessing and ultimately procuring systems to ensure that new systems can comply with this standard.
It is the responsibility of all holders of LSE IT accounts to adhere to the Standards described within this policy.
It is the responsibility of all staff and students to report cases that do not comply with this standard.
It is incumbent on all members of the School to communicate this policy.
The Information Security Manager will contribute to training materials to aid users in picking strong passwords.

Standard

Rationale

Passwords protect the confidentiality, integrity and availability of information at LSE. A password should be as long and complex as possible to thwart any brute-force attempts at guessing it. Its expiry is designed to limit both the length of time an attacker has to guess a given password and the length of time she can use a compromised password, i.e. the "window of opportunity".
The difficulty is that the longer and more complex the password, the greater the potential for forgetting it.

Password length

All passwords shall be a minimum of eight characters long. This is in line with industry best practice.

Password complexity

Passwords shall contain characters from at least three of the following five categories:

- English uppercase characters (A - Z)
- English lowercase characters (a - z)
- Base 10 digits (0 - 9)
- Non-alphanumeric (For example: !, $, #, or %)
- Unicode characters
- Cannot have the same first three characters as the username

Forced password change intervals

It is important to remember that all users should be able to change their passwords securely at any time, and more frequently than this schedule if they so wish.

Students

Students will be forced to be reset their passwords annually. It is proposed that this be incorporated into a "re-registration" page, where they can also re-confirm their agreement to the *Conditions of Use of IT facilities* at the LSE.

Everyone else

All other accounts will be required to change their password annually.

Additional controls

There are additional controls within Active Directory that will reinforce the password controls. Where these can be replicated in other systems, they should be.

Maximum retry count

The maximum number of incorrect attempts to input a password shall be limited to 5.

Retry count timeout

A time delay of 30 minutes shall be applied before the invalid password lockout count is reset to zero. (If a user attempts to login with an incorrect password more than 5 times in 30 minutes, then their account will be locked out)

Account lockout timeout

Accounts shall be locked out for 30 minutes before a new attempt can be made to input a password; this time period can be manually shortened via Support Staff intervention, having validated the identity of the user first: this internal IT Services process will be documented separately.

Password reuse settings

The re-use of the same password in less than eight cycles shall not be permitted.

Examples

Here are some valid passwords, according to the scheme above:

- H0llyTree
- SnowWh1te
- C0caC0la
- !WhistleStop!
- #W1ndsorCastle
- /*TerrysChocolateOrange*\

Exceptions (to this policy)

Due to the way in which these controls are implemented technically, there cannot be any exceptions to this policy for *users*.
However, there are some system-level accounts that are “hard-coded” into applications, which would have severe potential disruption to service if they are changed. Providing that these account very strong passwords that exceed the minimum standards described in this policy and there is adequate auditing of account access in place, such passwords may be allowed to never expire.

Appendix A Sign off form

Library reference: ISM-SD-009

Password Standard

Chair, Information Security Steering Group (who has delegated authority of ISSG to sign off LSE information security (or related) policy)**: Professor George Gaskell**

Signed: ..... *Date:*.....

Comments: .....

Chief Information Officer (The CIO is responsible for IT at LSE)**: Jean Sykes**

Signed: ..... *Date:*.....

Comments: .....

Assistant Director, IT Services - Technical Infrastructure) (with responsibility for Information Security and chair of the ICT Managers Group)**: Adrian Ellison**

Signed: ..... *Date:*.....

Comments: .....

Assistant Director, IT Services (MIS) (with responsibility for management information systems across LSE)**: Andy Coulthard**

Signed: ..... *Date:*.....

Comments: .....