Policy

LSE Password Policy

Jethro Perkins
Information Security Manager

Version	1.1
Date	15/10/15
Library reference	ISM-PY-002

Technical

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		
Alistair McGuire	Professor, Chair of LSE Health	LSE Health
Matthew Skellern	Project Manager	LSE Health

External document references

Title	Version	Date	Author
"Your LSE Password" http://www.lse.ac.uk/intranet/LSEServices/IMT/infosec/yourLsePassword.aspx	1	-	Jethro Perkins
Information Security Policy	3.7	01/07/15	Jethro Perkins

Version history

Date	Version	Comments
7/11/11	1.0	Release version (details on website as part of "Your LSE Password": http://www.lse.ac.uk/intranet/LSEServices/IMT/infosec/yourLsePassword.aspx)
15/10/15	1.1	Updated and placed into standard LSE IMT policy format to reflect HSCIC comments. Added in section 3.2 to explicitly refer to accounts used by persons with access to HSCIC-supplied data (where the required maximum expiry is 90 days)

Review control

Reviewer	Section	Comments	Actions agreed
HSCIC	-	No version history, no document control	Formalised using standard LSE Information Security Policy template
HSCIC	-	Password to accounts that have access to HSCIC-supplied Personally Identifiable Data must be changed <=90m days	Separate section introduced to deal with HSCIC-supplied data

Technical

Table of contents

Technical

1 Introduction

LSE passwords are the main way access to data is protected. It is therefore important to ensure that end users pick good passwords. Passwords need to be hard for hackers to crack, difficult to guess and changed periodically (in case a password becomes known over time).

LSE has a password policy in place for a number of reasons:

- Complex passwords are less easily guessed, meaning your LSE account is more secure and less likely to be hacked
- The expiry date means that if someone does have access to your account without you knowing it, that access will end when the passwords change
- IMT have a duty to provide you with systems that ensure a good level of security
- Using passwords that are complex and that expire has been recommended by our auditors as best practice
- Regular password expiries are explicitly required by some service and research data providers

1.1 Purpose

The password policy has been put in place to make sure passwords overall are stronger and data are safer.

1.2 Scope

All end user accounts. This includes staff, student and system accounts contained within Active Directory, supplier accounts and local accounts on systems.

Technical

2 Responsibilities

IMT Systems

- Implementing the policy across the LSE's Active Directory (AD).
- Maintaining different password policies within AD (1 year, 90 days, 30 days).
- Implementing supplier accounts, system accounts and service accounts.
- Resetting disabled accounts.

RLAB IT Manager
Implementing the policy for the RLAB Active Directory domain.

Information Security Manager
Responsible for this policy

System owners
Responsible for password policy implementation on non-AD systems.

Users
Keeping their passwords secure, implementing this policy on any LSE system where it is not enforced by technical controls, and not disclosing passwords to anybody.

Technical

3 Policy

3.1 Standard Duration

Passwords for standard LSE users (staff, students, associates) must be changed at least once per year.

All users will receive an email 30 days before expiry, and regularly thereafter, reminding them of the required password change.

3.2 Duration for accessing HSCIC Personally-Identifiable Data (PID)

Any user requiring access to HSCIC-supplied data will have their user account placed in a group where the maximum password duration is 90 days.

3.3 LSE Active Directory Domain Administrator accounts

LSE AD Domain Admin accounts have a maximum password duration of 30 days.

3.4 Password complexity

All LSE Passwords must:

- Be at least 8 characters long
- Contain at least one uppercase letter and at least one lower case letter
- Contain at least one number or punctuation character
- Include only characters supported on campus machines (avoid international characters)
- Not be a dictionary word

3.5 Non-compliance

Failure to change a password within the defined duration will lead to the account becoming disabled. This will require intervention from Information Management and Technology in order to re-enable the account.

3.6 Incident Handling

If a member of the School (staff or student) is aware of an information security incident then they must report it to the Information Management and Technology Service Desk at IT.Servicedesk@lse.ac.uk or telephone 020 7107 5000.

If necessary, members of the School can also use LSE's Whistle Blowing (Public Interest Disclosure) policy (see http://www2.lse.ac.uk/intranet/staff/brightIdeas/haveYourSay/whistleBlowing/Home.aspx.)

3.7 Review and Development

This policy, and any subsidiaries, shall be reviewed by the Information Security Advisory Board (ISAB) and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems