Lews Castle College UHI Password Policy Statement

Section 1 - Overview

Overview
Lews Castle College UHI’s intentions for publishing this policy are not to impose restrictions that are contrary to Lews Castle College UHI’s established culture of openness, trust and integrity. Lews Castle College UHI is committed to protecting Lews Castle College UHI’s partners, employees, students, and clients from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet / Intranet / Extranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network, accounts providing electronic mail, WWW browsing, and FTP, are the property of Lews Castle College UHI. These systems are to be used for business and educational purposes in serving the interests of the College and of our employees, students and clients in the course of normal operations.

Effective Information Security is a team effort involving the participation and support of every Lews Castle College employee, student and third party who deals with information and information systems.

It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

Scope
The scope of this policy includes all personnel, students or third parties who are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Lews Castle College UHI facility, has access to the Lews Castle College UHI network, or stores any non-public (Lews Castle College UHI) information.

Section 2 - Policy

2.1 General
a. All system-level passwords (e.g., root, enable, server admin., application administration accounts, etc.) must be changed on at least a quarterly basis.
b. All production system-level passwords must be part of the administered global password management database.
c. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
d. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
e. Passwords must not be inserted into email messages or other forms of electronic communication.
f. All user-level and system-level passwords must conform to the guidelines described below.
2.2 Guidelines

2.2.1 General Password Construction Guidelines

Passwords are used for various purposes at Lews Castle College UHI. Some of the more common uses include: User-level accounts, web accounts, email accounts, screen saver protection, voicemail password and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords, which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word that can be found in a dictionary (English or foreign)
- The password is in common usage, such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like qwerty, zxcvbnm, 789456, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*(_+|~-=\':;<>?)
- Are at least eight alpha-numeric characters long
- Are not in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can easily be remembered.

2.2.2 Password Protection Standards

- Do not use the same password for Lews Castle College UHI accounts as for other non-Lews Castle College UHI access (e.g., personal ISP account, Hotmail, etc.) Where possible, don’t use the same password for various Lews Castle College UHI access needs.
- Do not share Lews Castle College UHI passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Lews Castle College UHI information.
- Change passwords at least once every six months (except system-level passwords, which must be changed quarterly). The recommended change interval is every four months.
- If an account or password is suspected to have been compromised, report the incident to your manager and change all passwords.
- Password cracking or guessing may be performed on a periodic or random basis on Lews Castle College UHI IT systems. If a password is guessed or cracked during one of these scans, the user will be required to change it.
2.2.3 Use of Passwords and Passphrases for Remote Access Users

- Access to Lews Castle College UHI networks via remote access, i.e., VPN, is to be controlled using two-tier authentication.

2.3 Enforcement

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including, termination of employment.

Some password “don’ts”:

- Don’t reveal a password over the phone to ANYONE
- Don’t reveal a password in an email message
- Don’t reveal a password to your manager
- Don’t talk about a password in front of others
- Don’t hint at the format of a password (e.g., “my family name”)
- Don’t reveal a password on questionnaires or security forms
- Don’t share a password with family members
- Don’t reveal a password to co-workers when you go on vacation
- Don’t use the “Remember Password” feature of applications such as web browsers or email
- Don’t write passwords down or store them anywhere in your office
- Don’t store passwords in a file of ANY computer system without encryption

For Further Information Contact:
Danny Richardson
ICT Systems Manager
Tel: 01851 770262
Email: danny.richardson@uhi.ac.uk