Password Construction Guidelines

Password Construction Guidelines, version 1.0		
Status:	☐ Working Draft	☒ Approved
Document Owner:	Don Becchetti	
Last Review Date:	10/29/2024	

Password Construction Guidelines

Purpose

These guidelines aim to establish best practices for creating strong passwords.

Scope

These guidelines apply to all personnel using Lifeworks information technology resources, including employees, contractors, consultants, temporary staff, volunteers, and vendors. They cover all passwords for user-level accounts, system-level accounts, web accounts, email accounts, screen saver protection, voicemail, and network equipment accounts.

Statement of Guidelines

All passwords should meet or exceed the following standards. Password requirements extend to all internal and external systems related to Lifeworks business.

Strong Password Characteristics:

- At least 12 characters.
- At least 3 of the following character sets:
  - Uppercase letters
  - Lowercase letters (including spaces)
  - Numbers (0-9)
  - Special characters (!$%^&*()_+|~-=` {}[]:";'<>?,/)
- No more than two characters in a row from your username or full name.
- Spaces may be used in Lifeworks (e.g. Citrix XenApp, Microsoft 365) passwords.

Weak Password Characteristics:

- Fewer than 12 characters.
- Found in a dictionary or language slang.
- Contain personal information (e.g., birthdates, names).
- Include work-related information (e.g., Lifeworks names, system commands).
- Feature number patterns (e.g., aaabbb, qwerty).
- Use common variations like "Welcome123" or "Password123."

This information is available in an alternate format upon request.
Lifeworks is an Equal Opportunity Employer.

Passwords should not be written down. Passwords that are easily remembered should be used. Lifeworks Information Technology recommends using passphrases as a method to create easily remembered passwords that meet length and complexity requirements.

Passphrases

A passphrase is a longer password made of multiple words, offering greater security against attacks. Strong passphrases should follow the same guidelines as passwords and include upper and lowercase letters, numbers, and special characters.
Example of a strong passphrase (Do not use this exact example):

The Road To Succe$$ Is Fi11ed With Cha11enges

Compliance

The IT security will verify compliance through system checks, audits, monitoring, and feedback.

Non-Compliance

Violations may result in disciplinary action, including possible termination.

Exceptions

Any exceptions must be approved by the Director of Information Technology or VP of Information Technology in advance.

Definitions and Terms

None

Rights & Responsibilities

This section outlines expectations for everyone covered by these guidelines and the consequences for non-compliance.

Resources

- SANS Institute Information Security Policy Templates: SANS Institute
- Password Protection Policy

Version History

Version	Modified Date	Approved Date	Author	Reason/Comments
1.0	10/29/2024	10/29/2024	Don Becchetti	Original Document