PASSWORD PROTECTION POLICY

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

Table of Contents

..... 3
Overview 3
Purpose 3
Scope 3
Policy 3
- Password Creation 3
- Password Change 4
- Password Protection 4
- Application Development 5
- Use of Passwords and Passphrases 5

Policy Compliance 5
- Compliance 5
- Non-compliance 5

Related Standards, Policies, and Processes 6
Definitions and Terms 6
Version History 6

PASSWORD PROTECTION POLICY

Overview

Passwords play a crucial role in securing our information technology resources. Weak passwords can lead to unauthorized access and misuse of Lifeworks resources. All Lifeworks personnel (employees, contractors, consultants, temporary staff, volunteers, and vendors) are responsible for choosing and securing strong passwords.

Purpose

This policy establishes guidelines for creating strong passwords, protecting them, and determining how often they should be changed.

Scope

This policy applies to all personnel with user accounts or access that requires a password on any Lifeworks system. It also covers access to the Lifeworks network and any non-public Lifeworks information. Password requirements extend to all internal systems related to Lifeworks business.

Relevant Systems

- Simple Network Management Protocol (e.g., Routers, Switches, Firewalls, Access Points, Servers, Printers)
- Active Directory/Azure (e.g., Citrix desktops, Microsoft login, email)

Policy

Password Creation

- **Follow Password Construction Guidelines**: All passwords must adhere to the Password Construction Guidelines, which specify requirements for length, complexity, and character variety.
- **Avoid Reusing Personal Passwords**: Personnel must not use passwords from personal accounts, such as personal email or social media, for Lifeworks system access accounts.
- **Unique Passwords for Lifeworks Accounts**: To further enhance security, avoid using the same password for different Lifeworks accounts.

- **Unique Passwords for System-Level Privileges**: For accounts with system-level privileges, it is essential that these passwords are unique and distinct from all other passwords utilized by the system-level user.
- **SNMP Community Strings**: When using Simple Network Management Protocol (SNMP), community strings must be defined as something other than the standard defaults (e.g., “public,” “private,” and “system”).

Password Change

- System-level passwords must be changed at least once a year (e.g. root, enable, local and domain administrator, application administration accounts).
- Lifeworks passwords must be changed at least every 90 days.
- The IT team may conduct periodic password cracking checks. If your password is compromised, you must change it immediately.

Password Protection

- Never share Lifeworks passwords. No one (supervisors, coworkers, or IT staff) should ever ask for your password.
- Do not share your passwords via email, phone, or any form of electronic communication.
    - Information Technology may share initial or temporary passwords with you.
- Any initial or temporary password provided should be reset immediately.
- Passwords must not be written down or stored on devices. Consult IT if password storage is necessary for business purposes.
- Avoid using "Remember Password" features for Lifeworks accounts (e.g. web browsers).
- If you suspect your password has been compromised, report to IT immediately and change all relevant passwords.

Application Development

Developers must ensure that applications:

- Authenticate individual users, not groups.
- Do not store passwords in plain text.
- Do not transmit passwords in plain text over the network.
- Allow role management, enabling one user to take over another's functions without needing their password.

Use of Passwords and Passphrases

- Lifeworks recommends the use of passphrases. Passphrases are long combinations of words that are easier to remember. A strong passphrase should:
- Be long and include uppercase and lowercase letters, numbers, and special characters.
- Avoid easily guessed phrases.
- Example of a strong passphrase (do not use this exact example):
  The Road To Succe$$ Is Fi11ed With Cha11enges

Policy Compliance

Compliance

The IT security team will monitor compliance through system checks, audits, and feedback. Any exceptions to this policy must be approved in advance by the Director of Information Technology or VP of Information Technology.

Non-compliance

Violating this policy may result in disciplinary action, including possible termination.

Related Standards, Policies, and Processes

- Password Construction Guidelines

Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Simple Network Management Protocol (SNMP)
- Active Directory/Azure passwords (Citrix desktops, Microsoft login, email)
- Lifeworks Password (Citrix desktops, Microsoft login, email, Teams)

Version History

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