Password Policy

Purpose

The purpose of this policy is to ensure that only authorized users gain access to Nested Knowledge's information systems.

Scope

This policy affects all employees of this Nested Knowledge and its subsidiaries, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject to disciplinary action up to and including termination.

Affected Systems

This policy applies to all computer and communication systems owned or operated by Nested Knowledge and it's subsidiaries. Systems include company shared drives, purchased software, as well as access to the Nested Knowledge AutoLit review platform. Similarly, this policy applies to all platforms (operating systems) and all application systems. Reviews developed in the AutoLit software by parties external to Nested Knowledge are not covered in this policy.

Policy

Internal Company Passwords

Application Passwords - All programs, including applications developed internally by Nested Knowledge must be password protected.

Changing Passwords - All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.

Sharing Passwords - Passwords must be kept confidential and may not be shared among users. Users are prohibited from recording passwords in an unencrypted medium, like a notetaking application, mobile phone, or piece of paper. Company credentials, including work email and other work accounts, may NEVER be used on personal websites.

Password Storage - Passwords will not be stored in readable form without access control or in other locations where unauthorized persons might discover them. All such passwords are to be strictly controlled using either physical security or computer security controls

Password Complexity

Passwords must:

- be at least 12 characters long
- contain a mix of at least three of the following characters:
    - uppercase
    - lowercase
    - numeric
    - non-alphanumeric
- must not match your user name or email

Application Passwords

Application Passwords - All programs, including third party purchased software and applications developed internally by Nested Knowledge must be password protected.

User Authentication

All systems will require a valid user ID and password. All unnecessary operating system or application user IDs not assigned to an individual user will be deleted or disabled. The use of a four digit pin or secret questions is not acceptable as an authentication method.

As described in our Secure Development Policy, Nested Knowledge does not manage user passwords or authentication (handled by Auth0 and Auth0 Lock). All communications with Auth0 from the client are encrypted (TSL), ensuring passwords are not communicated in plain text. Passwords stored by Auth0 are similarly salted & encrypted (bcrypt). Communications relayed by the client are similarly encrypted & RSA signed.

Choosing Passwords

All user-chosen passwords must contain at least one alphabetic character, one number, and one special character. Passwords must contain a minimum of 8 characters. All users must be automatically forced to change their passwords appropriate to the classification level of information. To obtain a new password, a user must present suitable identification. Passwords requirements are set by the respective systems—for instance, Google Accounts and Outh2, and are subject to change.

General Password Guidelines

Applies to Nested Knowledge internal passwords and passwords for all Nested Knowledge users.

Password Expiration Time

The company does not currently have a Password Expiration Time policy; Google and Auth0 may require users to change their passwords at required intervals, but the company defers to these provider's policies with respect to password expiration.See https://auth0.com/docs/secure/attack-protection/brute-force-protection.

The company will review the Password Expiration Time policy periodically to ensure that long-term exposures are minimized.

Password Constraints

The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. After multiple unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three minutes, or © if dial-up or other external network connections are involved.

Changing Passwords

All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.

Sharing Passwords

Passwords must be kept confidential and may not be shared among users. Users are prohibited from recording passwords in an unencrypted medium, like a notetaking application, mobile phone, or piece of paper.

Revision History

Author	Date of Revision/Review	Comments/Description
K. Cowie	10/06/2023	Minor revisions
K. Kallmes	11/19/2021	Initial Draft approved
P. Olaniran	08/30/2022	Revised draft
K. Cowie	09/01/2022	Draft approved
K. Holub	01/26/2023	Added password complexity requirements

Return to Policies