Multi-Factor Authentication

I. Purpose

This policy outlines our plan for implementing advanced authentication of users who connect to Nested Knowledge information systems. We are committed to protecting the security, privacy, and integrity of Nested Knowledge information systems and personal and organization data, such as research data, intellectual property and financial information.

II. Scope

Who is affected: This policy affects all employees, contractors, consultants, and business partners of Nested Knowledge. **Affected Systems:** Server or VPN.

III. Policy

Nested Knowledge will implement multi-factor authentication (MFA) on an ad-hoc basis. We will evaluate the risk and sensitivity or personal and organizational data, such as personal employee data, user data, intellectual property, and financial information, on an ongoing basis. Evaluation will be based on our data classification system.

Communication

When a change in the scope or the nature of information handled by Nested Knowledge occurs, our technical and operational leads will alert the CTO that multi-factor authentication may be warranted. If client information is handled, a representative from the client organization will be included in discussions on MFA. After discussion and evaluation of security risks, the CTO will decide whether or not to implement multi-factor authentication.

Multi-Factor Authentication for Remote Access

Nested Knowledge has no internal network for employees, therefore multi-factor authentication for remote access is not applicable. Should Nested Knowledge establish a network, access to the network through remote access will be managed by a Virtual Private Network (VPN). The VPN will request for username and password, and may involve MFA.

Multi-Factor Authentication for Financial Information

At present, Nested Knowledge stores financial information via a cloud-based accounting software. Our security measures for protecting such data are determined by the software. At present, it requires MFA of all users. The accounting application is a VeriSign SecuredTM product, which is the leading secure sockets layer (SSL) Certificate Authority. It uses firewall protected servers and the encryption technology (128 bit SSL).

Authentication with Client Data

In cases where Nested Knowledge is granted access to client data, we will adhere to the level of authentication required by the client.

Revision History

Author	Date of Revision/Review	Comments
K. Cowie	11/24/2021	In progress.
K. Holub		
K. Kallmes		

From:
https://wiki.nested-knowledge.com/ - **Nested Knowledge**

Permanent link:
https://wiki.nested-knowledge.com/doku.php?id=wiki:policies:dualauth&rev=1637782672

Last update: **2021/11/24 19:37**