Mobile Device Policy

I. Purpose

The Mobile Device Policy exists to ensure that we protect from threats related to mobile devices.

I. Scope

This document offers guidance for employees and contractors working with Nested Knowledge.

II. Policy

Nested Knowledge does not provide employees or contractors with mobile cellular devices. Personnel are trained to avoid accessing confidential or sensitive data on their personal mobile devices. Our software application is not reccomended for use on mobile devices; functionality is highly limited.

Mobile Device Management:

Nested Knowledge employes a MDM solution to setup, monitor, and install updates on employee work-issued computers. We restrict admin priviledges to users who require root-level access due to development needs.

Use of Sidecar Displays:

On a case by case basis, employees may be authorized to use iPads or other mobile devices to extend their monitor display when necessary for work. Employees using sidecar displays must adhere to the following security measures:

1. Use a strong password, as defined in our password policy.
2. Use a security focused DNS Service in preference to automatic DNS settings
    1. Examples are Quad9, CloudFlare, or OpenDNS.
3. Install an adblocker on the device browser to protect from malware.

Support Contact Information

Name	Function	Contact
Karl Holub	Technical User Support	karl.holub@nested-knowledge.com
Jeffrey Johnson	Mobile Device Technical User Support	jeffrey.johnson@nested-knowledge.com

Revision History

We will update this policy as our equipment changes.

Author	Date of Revision/Review	Comments
K. Cowie	02/02/2024	Added Sidecar policy
K. Kallmes	11/19/2021	Draft approved
K. Cowie	01/24/2023	Reviewed

Return to Policies