Wireless Connection Policy

I. Purpose

Though the networks used by remote workers are beyond our control, it is essential that we mitigate these possible external threats as much as we can through this policy.

II. Scope

This policy applies to all employees and contractors who work with Nested Knowledge and access internal or confidential Nested Knowledge data.

III. Wireless Connection Policy

Wireless network acceptable practices are based on data classification. Public data may be accessed on any network. Internal Nested Knowledge data, confidential data, and restricted data may only be accessed on secure networks. All personnel accessing non-public data must avoid the use of public, high-risk networks.

Home Network Procedures:

All employess and contractors will be provided with guidance on procedures for safely using home networks, which includes practices such as using strong passwords, eliminating guest networks, securing IoT devices, and frequently updating devices.

Network Security Policy

I. Purpose

This policy provides guidance to safeguard networks from harm.

II. Scope

This policy applies to all employees and contractors who work with Nested Knowledge and access internal or confidential Nested Knowledge data.

III. Network Security Policy

Nested Knowledge, a fully remote company, does not maintain any internal networks for employees.

The Nested Knowledge cloud application, marketing site, and wiki run in an isolated, private network (Virtual Private Cloud, “VPC”). Only front-end servers are exposed to the internet via gateway; backend services and databases are unreachable outsde the VPC. Access to the VPC is provided by a bastion host via SSH key authentication; all access attempts to the bastion host are logged and periodically reviewed for unexpected or malicious activity.

Security protocols for the transmission of data across the network

All communications from the VPC are encrypted by SSH (developers) or HTTPS (users of the application). Within the VPC, communcations between all services and the database are encrypted via TSL.

Network change management procedures

When network architecture changes, a review by the technical lead, Karl Holub, must be processed. Additionally, the technical lead will perform annual review of this policy and ongoing compliance.

Revision History

Author	Date of Revision/Review	Comments
K. Cowie	11/15/2021	Initial draft partially complete; needs technical drafting
K. Kallmes		
K. Holub	11/17/2021	