Access Policy

I. Purpose

The purpose of this policy is to maintain an adequate level of security to protect Nested Knowledge data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of Nested Knowledge information systems.

II. Scope

Who is Affected: This policy affects all employees of this Nested Knowledge and its subsidiaries, and all contractors, consultants, temporary employees and business partners.

Affected Systems:

This policy applies to all computer and communication systems owned or operated by Nested Knowledge and its subsidiaries. Systems include employee computers, company shared drives, purchased software, as well as access to production software deployment environments. 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.

III. Access Control Policy

Entity Authentication

Any User (remote or internal), accessing Nested Knowledge networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- Automatic logoff
- Unique user identifier
- Password
- MFA device (Authenticator applications or physical device)
    - Dictated by MFA Policy

System Access Controls:

Access controls will be applied to all computer-resident information based on the class of the data and information to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

Administrative Privileges:

Access to Nested Knowledge Systems is managed by internal administrators who approve employees and contractors. For sensitive information, admin privileges are granted to limited personnel by company directors Existing administrators follow the Principle of Least Privilege (PoLP), per our Need-to-Know policy, when adding new administrators.

Need-to-Know:

Users will be granted access to systems and proprietary data on a need-to-know basis, following PoLP. That is, users or groups of users will only receive access to systems and information that are required for performing their job duties. If it's determined that a user or group needs access to a system or information, the access level (user vs. admin, read vs. write) is set according to the minimal set of information & actions needed in job duties. Job duties are identified by administrators granting access as those outlined in job description or, if not part of job description, written communication from a director.

Shared Accounts:

The use of shared credentials by Nested Knowledge employees and contractors is prohibited.

Removal of Users:

Individuals who are terminated, removed, or no longer in need of access to Nested Knowledge information systems will be removed from all systems within 24 hours in most cases, and within 72 hours under special circumstances.

Access for Non-Employees:

Individuals who are not employees, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use Nested Knowledge internal information systems unless the written approval of a Department Lead has been obtained. Before any third party or business partner is given access to this Nested Knowledge computers or internal information systems, a confidentiality, non-disclosure, or other similar agreement defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization.

Access for Law Enforcement and Authority:

Nested Knowledge will not disclose information unless:

- Making such a disclosure is a legal obligation, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved.

- A serious risk of imminent harm to individuals exists that justifies compliance with the Data Disclosure Requests

Request for data disclosure shall be immediately escalated to the Chief Technology Officer and the Information Security Team via email or Slack alert.

When the Data Disclosure Request is related to personal information of a Nested Knowledge Customer, Nested Knowledge will request that the Authority send the request directly to the customer. Should the Authority agree, Nested Knowledge will provide assistance to the customer so that they can fulfill the Request.

Unauthorized Access:

Employees are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. Quarterly review and automated alerting will enforce.

Access Reviews:

Nested Knowledge will perform quarterly access reviews on accounts for all inventoried systems, including but not limited to:

- Cloud services providers (AWS)
- Cloud-based applications (Hubspot, Gitlab, etc.)
- Google GSuite (mail, drive, meets, etc.)
- Social media accounts
- Company-issued devices (laptops)

Network Devices

Nested Knowledge does not manage network devices, which are handle by AWS.

IV. Audit Trails and Logging

Logging and auditing trails are based on the Data Classification of the systems. For confidential systems, access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account
- Method of access

All privileged commands must be traceable to specific user accounts. Audit trails for confidential systems should be backed up and stored in accordance with Nested Knowledge back-up and disaster recovery plans. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. All logs will be audited on a quarterly basis.

Methods of Audit Logs

Security incidents are logged by firewalls, servers, anti-virus solutions, intrusion detections systems, applications, and databases. Audits are performed by automated tools where provided, else manual review.

Frequency of Audit Logs

Audit logs are reviewed quarterly or ad-hoc; logs are retained for one year. We examine the data types collected from end users to ensure compliance with privacy laws and regulations.

V. Remote Access Policy

Remote Access (application):

The Nested Knowledge application is run in a VPC (for details, see Network Security Policy). This network is only accessible by release engineers who are granted SSH keys. These keys may be revoked or refreshed at any time, as necessitated by personnel changes or incidents.The VPC is only accessible through a single bastion host. Every access to the production environment configuration results in alert emails to release engineers & engineering management.

Remote Access (internal):

Nested Knowledge has no internal network for employees, therefore 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 or some other form of advanced authentication. Remote access must conform at least minimally to all statutory requirements including but not limited to HCFA and HRS-323C.

Workstation Access Control System:

All workstations used for this business activity, no matter where they are located, must use an access control system approved by Nested Knowledge. Employees must use company-issued devices for completing their work. Active workstations are not to be left unattended for prolonged periods of time, where appropriate, which is enforced through MDM. When a user leaves a workstation, that user is expected to properly log out of all applications and networks, and remove confidential information from desks, printers, and faxes. Users should avoid use of public charging stations and internet access.

When accessing Nested Knowledge systems, authorized users are responsible for preventing access to any of our computer resources or data by non-authorized Users. The authorized user bears responsibility for and consequences of misuse of the authorized user’s access.

Remote Working Environmental Controls:

Equipment should be located and/or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. At a minimum, remote employees must:

- Update default router administrator password
  - Following our Password Policy
- Disable remote access to the router
- Enable wireless encription (WPA2/3) on their home network
- Store company devices behind locked doors

Employees will be trained upon hire and updated on an annual basis. For cloud-related access protocols, please refer to our Cloud Security Policy.

Compliance Statement

All Employees and Contractors who access Nested Knowledge's information systems will be provided with and required to review the Remote Access Policy. Employees who deliberately violate this policy will be subject to disciplinary action up to and including termination.

Revision History

Author	Date of Revision/Review	Comments
K. Holub	9/28/2023	Annual Review
K. Kallmes	1/20/2022	Approved; removed chain of trust language
P. Olaniran	10/6/2022	Minor revisions
K. Cowie	01/24/2023	Minor revisions to workstation policy

Return to Policies