

Security Awareness Training Policies

I. Purpose

Nested Knowledge has a responsibility to educate our personnel on security practices and to comply with federal regulations related to Information Security awareness. This policy describes our plan to educate users on the importance of security.

II. Scope

This policy affects all employees, contractors, and consultants of Nested Knowledge.

III. Security Awareness Training Policy

Nested Knowledge distributes security policies to all employees and contractors as part of their training. When policies are updated, we ensure that all employees have ready access to the most recent version. All employees with roles in incident response, data protection, or data recovery must sign off on the corresponding policy. We require all remote employees to review the remote access policy.

IV. Data Protection Training Policy

Employee training requirements are based on the [data classification system](#). All employees and contractors will be provided with our data protection policy. Those who deal with confidential data, restricted use data, or high-risk personal data will be required to demonstrate understanding of our data protection procedures.

V. Enforcement

Employees who fail to review and comply with our information security policies, including the access control and incident management policy, will be issued a warning and required to demonstrate comprehension of security rules and procedures. Continued failure may result in disciplinary action.

Revision History

Author	Date of Revision/Review	Comments
K. Cowie	12/15/2021	Draft Completed
K. Holub		
K. Kallmes		

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

Permanent link:
https://wiki.nested-knowledge.com/doku.php?id=wiki:policies:security_training&rev=1639628012

Last update: **2021/12/16 04:13**