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.

Developer Training

Developers are expected to be familiar with common vulnerabilities in web applications, how to detect them, and how to mitigate them. To standardize this expectation, OWASP modules & guidelines are trained. Specifically:

- All developers perform an annual review of the OWASP Top 10 and pass a practical quiz relating to vulnerabilities within.
- Each developer annually completes a randomly selected test from the OWASP Web Security Testing Guidelines (WSTG) on the Nested Knowledge software
    - Scenarios will be selected and assigned by the Technical Lead using our issue management software
    - Each scenario includes a description of the threat, and testing methods. The developer inventories surface area, and performs a test/penetration in a development environment, as applicable.
    - The developer writes up their approach & findings in the issue, which is then reviewed by the technical lead.
- Any developer introducing a vulnerability identified in code review or later is expected to:
    - Study the corresponding OWASP Cheat Sheet(s), when relevant.
    - Demonstrate understanding of the threat to the technical lead, with regards to both the code instance and the general threat model.
    - With the technical lead, perform a review of relevant code examples in the code base and explain the mitigations used.

- OWASP Global AppSec training & webinar attendance is assigned on a discretionary basis (by the technical lead) for developers failing to achieve & demonstrate expected understanding of the above materials and exercises, or junior members of the team.

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.

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	
K. Holub	1/25/2023	Updated Dev Security Training Practices

Return to Policies