Purpose

The purpose of this policy is to identify the regulatory requirements for <Company> information assets through vulnerability management. And to define the measures for notification, testing, and installation of security patches on devices connected to <Company> networks, mitigate or remediate vulnerabilities.

Scope

This policy applies to all <Company> employees, contractors, third parties who access internal information and business processes.

Responsibilities

ISMS Manager:

Manage vulnerability and patch management processes.

SOC Analyst:

Regularly monitor the network and corporate devices for vulnerabilities;

Monitor the network for vulnerabilities.

Security Engineer:

Set up the vulnerability management agents on the network equipment;

Continuously improve the security system.

Asset Manager

Set up the vulnerability management agents on the endpoints.

Policy

Vulnerability Management Workflow

Vulnerability scanning

<Company> has to conduct routine scans of the company devices and servers connected to the network to identify all types of vulnerabilities biweekly or when any significant change is done.

The vulnerability scans are done with a corporate vulnerability scanner for all Windows, macOS, and Linux systems. The corporate vulnerability scanner is linked to SIEM for further monitoring and comparison. Also, it should compare the results of the current scan with the previous ones.

Vulnerabilities are regularly reviewed, evaluated, tested, and mitigated.

The critical or high vulnerability scan results must be remediated as soon as possible. Then the next session of scanning will be held to make sure that these vulnerabilities are closed.

The medium, low or informational vulnerabilities should be remediated at earliest convenience and due risk acceptance model

The dedicated account for vulnerability scans must be used for that activity explicitly.

The scan data is sensitive and mustn't be shared with people who are not involved in these processes.

The staff is strictly prohibited from making any temporary changes to the information system to pass an assessment successfully. <Company> Disciplinary Procedure will deal with any attempts to tamper with scan results.

When the system has vulnerabilities that can not be remediated, the Risk Assessment will be done to identify how these vulnerabilities can be mitigated. The corresponding security measures will be implemented.

Penetration testing

<Company> has to conduct penetration testing of the company devices and servers connected to the network to identify all types of vulnerabilities biannually or when any significant change is done.

Testing should exclude DoS, DDoS, and Brute Force and does not impact the <Company> systems' productivity.

Penetration testing should be conducted for finding vulnerabilities in the internal network and environments, which are segmented for Management, <Other departments>, and external (e.g., Website, etc.).

The penetration test data is sensitive and mustn't be shared with people who are not involved in these processes.

Remediation measures implementation

The planned remediating actions should be executed in line with the agreed deadlines.

If a problem occurs with implemented remediation, it should be recorded.

Alternative actions should be defined by the asset owner based on recommendations. These new or other remediating actions should then be implemented.

Rescan/Re-test

Once a vulnerability is remediated, a rescan/re-test has to be scheduled to verify the remediating actions have been implemented.

Patch Management

Asset Manager maintains overall responsibility for patch management implementation, operations, and procedures.

All resources must be scanned regularly to identify missing updates.

All missing software updates must be evaluated according to the risk they pose. Missing software updates that pose an unacceptable risk to <Company’s> resources must be implemented within a time that is commensurate with the risk.

Software updates and configuration changes applied to company systems must be tested before widespread implementation and must be implemented under the <Company> Change Management Policy.

Verification of successful software update deployment will be conducted within a reasonable time.