Removable media policy

1. Definitions and Terms

Encryption: Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Malware: A generic term for a number of different types of malicious code.

Removable Media: A form of computer storage that is designed to be inserted and removed from a system (examples: Optical discs, CompactFlash cards, USB Flash drive, ...)

Sensitive Information: Any unclassified information that, if compromised, could affect a company business.

2. Object

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

3. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by noesya and to reduce the risk of acquiring malware infections on computers operated by noesya.

4. Scope

This policy covers all computers and servers operating in noesya.

5. Policy

noesya staff may only use noesya removable media in their work computers.

noesya removable media may not be connected to or used in computers that are not owned or leased by noesya without explicit permission of the noesya security staff.

Sensitive information should not be stored on removable media.

No exception to this policy may be requested.

6. Policy Compliance

6.1. Compliance Measurement

The security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, internal audits, and feedback to the policy owner.

6.2. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7. Revision History

1.0 Date of change: 01/09/2021 - Responsible: Technical team - Summary of Change: Initial release