

Purpose

This policy describes the way we see using any type of removable media in our company. The purpose is to minimize the risk of loss or exposure of the company's information maintained by .

Scope

This policy applies to all employees, users, and third parties who access or use information assets, regardless of physical location.

IT resources include all company-owned, licensed, leased, or managed hardware and software used by the Infosec network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

Policy

Removable media usage is strictly prohibited (except if it is explicitly allowed by the Management), as it poses a high risk of malware infections or corporate data loss.

The only way of the applied data transfer is . Employees cannot download any type of received data on the USB drive or any other removable media.

The exception is Asset Manager, who can sometimes use the approved USB Drive for installation purposes.

Employees can ask for individual exceptions from the Management.