USB Flash Drive Security

Recommendations and Best Practices

Risks

USB flash drives or thumb drives pose a severe security risk to networks and data. Hackers can use them to transmit viruses and other malware every time they are plugged into another computer. Attackers may also use USB drives to steal sensitive information. USB drives are also easily lost or stolen. If the data was not backed up, the loss of a USB drive can mean hours of lost work. If the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it, potentially causing a data breach or leak Personally Identifiable Information (PII).

Recommendations

Staff are encouraged, and possibly required, to use authorized removable media with their devices for work-related functions. Sensitive information generally should not be stored on removable media in order to mitigate the risks mentioned above. If use of removable media is required for their work, it should be encrypted and placed only on officially registered removable media devices.

Best Practices

- Use Office365 OneDrive or another cloud backup service to securely store and access data. This also protects against potential data loss when the loss of a removable device.
- If you must use a USB drive, use passwords and encryption to protect the data.
- Keep personal and business USB drives separate - Do not use personal USB drives on computers owned by the organization, and do not plug USB drives containing work information into a personal computer.
- Use and maintain security software, and keep all software up to date - Use anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions current.
- Keep the software on a computer up to date by applying any necessary patches.
- Do not insert a USB device into a computer you don't trust.
- Do not plug an unknown USB drive into your computer. Instead, hand it over to your IT Department.