Information Technology
Archdiocese of Atlanta

USB Storage Device Exception Waiver

Why is access to USB Storage devices restricted?

USB storage devices, especially USB flash drives and hard drives, are notorious among hackers due to the inexpensive cost and portability. Plugging a USB storage device into an Archdiocese of Atlanta (AoA)-owned workstations can jeopardize the security posture of the AoA systems and data. The USB storage devices are one of the easiest channels to spread an infection to a workstation and/or network.

Disabling USB storage devices also discourages the use and storing of unencrypted data on flash drives and external hard drives. USB drives are small and easy to lose. If data is unencrypted, the data is easily accessible to non-authorized individuals. Therefore, those granted authorized USB Storage device access are encouraged to always use encryption on their external devices.

Dangers of USB Storage Devices

- The deliberate (or undeliberate) transferring of confidential AoA-owned data to personal USB flash or external hard drives.
- The unencrypted storing of data on USB flash or external hard drives.
- Inadvertently transferring malicious files to AoA-owned workstation.
- Plugging in USB storage devices found on the ground or handed out for free. USB storage devices, especially the ones found on the ground or handed out for free, can contain malware that can infect the workstation. It is common for hackers to use this method to install malware on victim's workstations. Once installed, the malware can perform a variety of malicious acts such as capturing keystrokes on your keyboard and encrypting your hard drive. The hacker can ask for ransom or spread the malware from one computer to the next, gradually infecting many, if not all, workstations.

How to Request a USB Storage Device Exception

For audit purposes, AoA must retain documentation showing that USB storage devices exceptions are approved and documented. To request an exception, an AoA employee must follow these steps:

1. Read this USB storage device exception waiver and understand the responsibilities of being granted access to the USB ports on your computer.
2. Complete and sign the sections below.
3. Submit a scanned (.PDF) copy of this form to the IT help desk at https://help.archatl.com

REQUESTOR INFORMATION	
NAME *(please print)*:	
DEPT:	
EMAIL:	
PHONE:	
BUSINESS JUSTIFICATION FOR REQUEST:	

SIGNATURE OF REQUESTOR	DATE		SIGNATURE OF DEPARTMENT HEAD	DATE

May 2024