Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● *The USB owner's name is Jorge is personally identifiable information (PII)* ● *Resume, Photo, Contract, and Employee files are sensitive personally identifiable information (SPII)* *Summary: This is absolutely unsafe because no access protection Thus, attackers can manipulate personal files. and work files can be accessed easily.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *The information can be used against other employees, the relatives and can be used to access the business.* ● *This can be used as a scam to get more information from relatives and family or hospitals.* ● *Can insert a suspicious program lurking on the USB and have Jorge put it back into the workstation again.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *Isolation: The use of virtualization software is a good mitigation step, as it allows the security team to investigate the USB stick in an isolated environment that is not connected to other files or networks.* ● *Scanning: Before opening any files on the USB stick, it's essential to conduct a thorough antivirus scan to detect and eliminate any potential malware.* ● *Restricted Access: Ensure that the investigation is carried out by knowledgeable and trained members of the security team to minimize the risk of accidental exposure to malware.* ● *Backup: Before investigating the USB stick, back up the workstation's data to ensure that any potential infection can be isolated and removed if necessary.*