Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● *Are there files that can contain PII?* ● *Are there sensitive work files?* ● *Is it safe to store personal files with work files?* *The files on the USB stick seem to be a mixture of personal and professional ones. A new hire letter and an employee shift schedule are both work-related documents, but family and pet images are of a more private nature. While the employee shift schedule and new hire letter may not directly contain personally identifiable information (PII) or sensitive work-related information, the personal images may indirectly contain sensitive information. It may not be the safest practice to save both personal and professional files on the same device because doing so increases the possibility of unintentionally exposing critical work data to security risks.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *Could the information be used against other employees?* ● *Could the information be used against relatives?* ● *Could the information provide access to the business?* *The information on the USB device might be utilized against Jorge, the hospital, other staff, or even Jorge's family members. On the drive, there are personal and professional documents that might be used to create social engineering or phishing scams against Jorge or other workers. The availability of a new hiring letter and an employee schedule may facilitate impersonation efforts, giving malicious actors access to the hospital's facilities or systems without authorization. Further social engineering attempts might target Jorge's loved ones if private information about relatives and family images are exploited. All things considered, the data on the USB drive presents a complex threat that might open up a number of attack vectors against both people and the hospital's security.*

Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* ● *What sensitive information could a threat actor find on a device like this?* ● *How might that information be used against an individual or an organization?* *The USB device discovered in the parking lot in this case may include a variety of harmful software, such as viruses, trojans, ransomware, or keyloggers. Another employee would unintentionally put malware into the hospital's network if the device were infected and they found out, which could result in illegal access, data breaches, or even the compromising of crucial systems.* *Personal and professional files belonging to Jorge Bailey, such as family and pet images, a new employment letter, and an employee shift schedule, could contain sensitive information that a threat actor could discover. Both an individual and an organization could be harmed by this knowledge. For Jorge, the exposure of personal photos might lead to privacy breaches, while work-related documents like new hire letters and employee schedules could be exploited by attackers for social engineering attacks, identity theft, or targeted phishing campaigns.*