# Parking Lot USB Exercise

| | |
|---|---|
| **Contents** | Write **2-3 sentences** about the types of information found on this device.<br><br>*The types of information found on the USB contain both personal and work-related information. Some files contain Jorge's wedding list, vacation ideas, dog photos, and his resume. As well as work-related files like shift schedules, the employee budget, and a new hire letter. It is not safe to store personal files and work files together, especially if they're this sensitive to a person's identity.* |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.<br><br>*This information could be used against the business, Jorge's relatives, and other employees. There's information about shift schedules, the employee budget, and Jorge himself. An attacker could use the information to exploit plenty of vulnerabilities personally to Jorge as well as the employees at the company as well.* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:<br><br>*There could be malware like a virus, worm, spyware, ransomware, or a rootkit on the USB. If the USB was picked up by a different employee and they plugged it into their work device, there could have been major consequences. A threat actor could find anything from PII, SPIII, or PHI on a USB device like this about someone or a group of people. It could be used against an individual or an organization by containing sensitive information and allowing an exploit from that. It could be something personal that may be blackmailed or against an entire organization's reputation.* |