# Parking lot USB exercise

| | |
|---|---|
| **Contents** | Write **2-3 sentences** about the types of information found on this device.<br>● *Are there files that can contain PII?*<br>● *Are there sensitive work files?*<br>● *Is it safe to store personal files with work files?*<br><br>● *The flash drive has a mix of highly sensitive personal and work-related files that should be separated.*<br>● *Personal files contain family/pet pictures, Jorge's resume, a vacation planner, and a wedding list.*<br>● *The work files contain hospital shift schedules, employee budgets, and a new hire letter template.* |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.<br>● *Could the information be used against other employees?*<br>● *Could the information be used against relatives?*<br>● *Could the information provide access to the business?*<br><br>● *It could have been a decoy for Jorge or a coworker to find and plug into a hospital computer to install malware.*<br>● *There is a chance the personal files weren't backed up and would be lost if anyone stole the USB drive.*<br>● *A threat could use the new hire letter and shift schedule to impersonate a new employee to access the hospital resources.* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:<br>● *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?*<br>● *What sensitive information could a threat actor find on a device like this?*<br>● *How might that information be used against an individual or an organization?*<br><br>● *The hospital should add a policy to keep personal files off their business USB to decrease the chances of workers taking and losing them.*<br>● *Add passwords and encryption to all business USBs to* |

| | |
|---|---|
| | *protect their sensitive data.*<br>● *Update and maintain the hospital's security software to defend against viruses and malware.* |