## **Parking lot USB exercise**

| **Contents** | Write 2-3 sentences about the types of information found on this device.  The USB contains both personal and work-related files belonging to HR manager Jorge Bailey, including family photos and HR documents like a new hire letter and an employee shift schedule. These files contain personally identifiable information (PII), making the device highly sensitive and vulnerable to misuse if accessed by unauthorized individuals |
| --- | --- |
| **Attacker mindset** | Write 2-3 sentences about how this information could be used  against Jorge or the hospital.  An attacker could have planted the USB drive as bait, hoping hospital staff would plug it in out of curiosity. The mix of personal and work files might distract the user, while hidden malware quietly opens a backdoor into hospital systems. With physical access, the attacker could also use the USB to steal sensitive data directly from a workstation |
| **Risk analysis** | Write 3 or 4 sentences describing technical, operational, or managerial controls that could mitigate these types of attacks:  Even without malware, this USB posed a serious security threat. It stored personal and operational data that could be used to target Jorge or compromise the hospital. If infected and plugged in, it could spread ransomware, leak files, or grant unauthorized access. To prevent attacks like this, staff should be trained to handle unknown devices, USB ports should be restricted, and work and personal data should always be stored separately. |