## **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 USB device may contain files with Personally Identifiable Information (PII), such as patient records or employee details, and sensitive work files like confidential hospital reports or access credentials. Storing personal files with work files is not safe, as it increases the risk of data breaches and potential malware contamination, compromising both personal and work data.* |
| **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 could be used against Jorge or the hospital by exploiting sensitive data, such as PII, to carry out identity theft or phishing attacks. If the data includes employee records, other employees could become targets, and attackers might use personal information to manipulate or harm their relatives. Access credentials or internal files could also provide a gateway for attackers to breach the hospital's systems, jeopardizing its security and operations.* |
| **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?*   *Malicious software like ransomware, keyloggers, or Trojans could be hidden on the USB device. If infected and accessed by another employee, the malware could spread through the network, causing data breaches, system lockouts, or stolen credentials. Sensitive information such as patient records, employee details, or access credentials could be found and used for identity theft, phishing, or unauthorized system access. To mitigate these risks, technical controls like USB scanning tools and network segmentation should be implemented, while operational policies such as employee training on handling unknown devices and incident reporting can strengthen the organization’s defenses.* |