## **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 drive contained a mix of personal and work files. Personal files included photos of family and pets, a vacation ideas document, a guest list document, and the owner’s resume. The driver also contained work files including a new hire letter, a shift schedule, and a budget document.  Both personal and work files contain PII such as the personal resume, the new hire letter, and the shift schedule. Personal and work files should not be mixed as it is unsafe and a security risk. |
| --- | --- |
| **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 in the work documents could be used to identify or potentially contact employees. The personal photos, vacation ideas, and guest list could be used to identify and potentially locate and/or contact relatives. The work schedule could potentially be used to determine times to attempt unauthorized access to the business. The new hire letter and budget document could be used to impersonate an employee or in a social engineering attack (by pretending to be authorized to receive information by knowing other business information). |
| **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?*   Training should be provided warning of the dangers of found USB devices. Policies should be in place prohibiting the attachment of unauthorized USB devices. The network should be monitored for unauthorized USB devices. Network policies should be in place to prohibit access to unauthorized USB devices. Policies should prohibit mixing personal and work files. Policies should require the encryption of PII. Policies should require the encryption of company data on removable storage. |