## **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?*   There are files that contain Personally Identifiable Information on the USB drive. There are also work files that should not be exposed to anyone such as resume, project or event management files, application letter, budget proposals, and photos of biometrics and facial features. It is highly encouraged not to store personal files with work files. Aside from organization purposes, work files should be separated for security purposes such as protecting intellectual properties, customer data, and employer and employee 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?*   For the other employees, the information collected from the USB drive can be utilized to digital crimes such as using someone’s address and contact number for fake delivery of goods, using signature for signing documents without a permission to the owner of it, and contact number for conducting social engineering attacks through calls. These incidents are also applicable to the relatives and business. Additionally, business company or the hospital itself may suffer from injection attacks, malicious softwares, and identity based attacks when the USB drive is returned or utilized again. |
| **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?*   When an unauthorized flash drive or USB drive is inserted in a device out of curiosity, the risk is high. A certain USB drive might have a malicious code that will be executed when inserted in a device. This can be a virus, where the files can be infected. The USB drive can also be utilized as a hardware that is connected to the hacker, such as a keyboard or a webcam that monitors the activity of the user. One example is the Rubby-Ducky, wherein a predefined keyboard key will be pressed to execute the malicious code inside the USB drive. These malicious codes can access the unprotected files where the USB drive is inserted, and the important information such as personal records that contain full name, address, contact number, medical history, financial transactions, and business acumens will be utilized for criminal activities. Promoting awareness to the employee, installing antivirus software and firewall, and disabling autoplay are the precautionary measures that can be conducted for mitigating the attacks stated above. |