Parking Lot USB Exercise Project

Contents	The USB device may contain various types of information, including files with Personally Identifiable Information (PII) such as employee details, sensitive work files like confidential reports or project plans, and potentially even malicious content. Storing personal files alongside work files is not recommended, as it increases the risk of security breaches and data contamination. Mixing personal and professional data can compromise both personal privacy and organizational security, violating IT policies.
Attacker mindset	The information on the USB could be exploited to harm employees, such as using PII for identity theft or phishing attacks targeting colleagues. Sensitive details might also expose relatives to scams or social engineering. Additionally, work files could provide attackers with access to critical business systems, intellectual property, or confidential strategies, potentially leading to financial loss, reputational damage, or legal liabilities.
Risk analysis	To mitigate such attacks, organizations can implement **technical controls** like USB port management, endpoint detection systems, and automatic scanning of connected devices for malware. These measures can help prevent infections from malicious software, such as keyloggers, ransomware, or spyware, which could compromise both individual and organizational data. **Operational controls** include mandatory training for employees to recognize and avoid using untrusted USB devices and clear procedures for reporting found devices. Additionally, **managerial controls** like enforcing strict data classification policies and limiting access to sensitive information can minimize the risks of data exposure, reducing the potential for exploitation by threat actors.