|  |  |
| --- | --- |
| Prepared by: | Marvellous Onuma-Kalu |
| Date: | 01/08/2024 |

|  |
| --- |
| **Physical Control Recommendations** |
| Given the nature of COMPANY\_A’s business and its location at an office park that is home to 3-4 similarly sized companies with shared parking facilities, here are some physical control recommendations to enhance security:   * **Access Control Systems**: Implement a robust access control system for the main office entrance and sensitive areas within the facility. This may include key card access or biometric systems to restrict entry only to authorized personnel. * **Security Cameras**: Install surveillance cameras at key points around the office park. This can deter unauthorized access and provide valuable footage in case of incidents. * **Lighting**: Building exteriors and parking areas should be well-lit during non-business hours. This is a simple yet effective deterrent against criminal activities. * **Security Guards**: Employ security guards to monitor the premises, especially during non-working hours. This can deter potential intruders and provide a quick response to any security issues. * **Secure Storage Areas**: Storage areas for valuable assets or sensitive information should be properly secured with additional access controls and monitoring. * **Visitor Management System**: This should be implemented to track and control the entry of guests into the office. This process could include sign-in processes, badges, and escorting procedures for visitors |
| **Logical Control Recommendations** |
| Logical controls are mechanisms that protect information assets with rules about how data is accessed, transmitted, processed, and stored within the context of a system or application. The following would be recommended:   * To achieve a secure architecture, we would add a firewall before the DMZ, in addition to the firewall that is installed before the LAN. * Add an Intrusion Detection System (IDS) behind the firewall on the edge of the network. * Website should be configured to use HTTPS (SSL/TLS) to encrypt data transmitted between clients and the API server, given that it handles eCommerce. This helps prevent data interception, man-in-the-middle-attacks, and ensure confidentiality and integrity of communication. * Ensure a robust API security strategy is implemented by following security standards and best practices. * Limit potential attacks on databases by deploying a database firewall to monitor and filter database traffic, enabling database auditing to track log activities. |
| **Administrative Control Recommendations** |
| See the attached documents, they contain administrative control recommendations.   * Company\_A – Password-Protection-Policy.docx * Company\_A – Remote-Access-Policy.docx |