|  |  |
| --- | --- |
| Prepared by: | **THIORO FALL** |
| Date: | **7/08/2021** |

|  |
| --- |
| **Physical Control Recommendations** |
| 1. **Protective Barriers** - mechanisms that provide a physical barrier are often the outermost layer of security. Example: **man traps**   Man-trap prevent unauthorize access to the building.  Install man-trap on each entrance of the Company A building.   1. **Antitheft devices**   May Include combination safes, cables/locks for equipment, cable alarms serve to **detect in order to protect the Company assets.**  **The Company should implement enough antitheft devices** in the building. |
| **Logical Control Recommendations** |
| 1. **Antivirus and Anti-Malware Software**   **Anti-virus and anti-malware software** can detect and remove malicious software.  The Company should install **antivirus and anti-malware software** on each host in network.   1. **Multi-factor authentication**   Which grant access to a resource after verification with two or more authentications factor.  The Company A should require a **multi-facto authentication.** |
| **Administrative Control Recommendations**   1. **Procedure**   A set of documents that address mandatory practices.  There are the most detailed security documents as they list what steps should be followed in order to meet the objective in the policy, standard, and baselines.  The Company A can implement a set of procedure rules that direct the organization.   1. **Policy**   A set of principles and rules Example: “Data must be encrypted”  Policies are essentially the law of the land and are considered mandatory.  The Company A can implement a set of policy rules that direct the organization. |
| ***Acceptable Use Policy***  ***Acceptable Encryption policy*** |