|  |  |
| --- | --- |
| Prepared by: | Arwa AlQadheeb |
| Date: | Saturday, October 15, 2022 |

|  |
| --- |
| Physical Control Recommendations |
| 1. Place Closed Circuit Television (CCTV) to deter potential intruders from gaining unauthorized access to COMPANY\_A premises. Also, CCTVs can be used to discourage unauthorized employees from piggybacking authorized employee into restricted areas (e.g., spaces that houses sensitive hardware). CCTVs will be placed all around and within COMPANY\_A premises (i.e., premises entrance, hallways, common spaces, office spaces and so on, excluding washrooms) and support 24/7 continuous recording to collect evidence in case of criminal activities. 2. Install **Biometric Smart Terminal + Door Sensor** (e.g.,[ZKTeco IN05 & IN05-A](https://www.zkteco.com/en/IN05_Series/IN05-IN05-A)) instead of traditional locks, which scan and verify employee’s fingerprint before granting them access to specific area. By doing so, security risks that result from lost, shared, copied, and stolen keys can be eliminated. In addition, it will restrict access to prohibited areas only to those who are authorized. Biometric Smart Terminals + Door Sensors will be placed on what is considered restricted area within COMPANY\_A and will be connected to its corresponding software to keep track of who access the room and when. |
| Logical Control Recommendations |
| 1. Encrypt all types of data (i. e., customers information, staff information, financial information, etc.) while being stored or exchanged between different components of the information system. By converting plain text into encrypted text, we ensure that data on our information system is secured and only accessible by those employees who have the appropriate privilege to do so. In addition, in case of a data breach, we ensure that data of our customers, staff, and intellectual property are not given on silver platter to criminal individuals. For instance, we use **Symmetric Cryptographic** algorithm to encrypt data stored on our file server that is sensitive and valuable, containing, for example, legacy data that is stored as series of Excel spreadsheets where it must be scrambled and unreadable by humans. Moreover, we ensure that emails, containing sensitive data, are exchanged between employees in a secure manner using **Asymmetric Cryptographic** algorithm. Encryption within COMPANY\_A is a must not an option. 2. Deploy additional external firewall to protect our perimeter network that is a buffer zone (aka Demilitarized Zone – DMZ) between the outside internet and our internal network. The firewall will filter and control the flow of internet traffic to protect our DMZ by blocking unwanted incoming traffic. By having dual firewall (i.e., external firewall and internal firewall), we will add extra layer of protection that only allow genuine traffic to enter DMZ by using **Stateful Network-Layer Firewall**, which is provided by different vendor than the one of the internal. Dual firewall from different vendors will eliminate the chance of having the same vulnerability, if exists, on different network components. Consequently, attackers will struggle and spend more time and effort to break into our information system. |
| Administrative Control Recommendations |
| * Acceptable Use Policy. * Password Protection Policy.   SANS Institute 2014 – All Rights Reserved |