|  |  |
| --- | --- |
| Prepared by: | Shrividya Ranjani Kaliyur NarayanaPrasad |
| Date: | 2/26/2021 |

|  |
| --- |
| Physical Control Recommendations |
| Use of Biometrics as a factor of authenticating the staff. Staff members entering the office building must provide some physical proof that he/she is who they claim to be. To fulfill this, biometrics like fingerprint, voice or retina scan must be done. This ensures that only authorized personal can access the data. This ensures that on authorized personal in entering the building and none of the unauthorized personal is entering the building. This reduces the risk of authorized material access and data leak. |
| Logical Control Recommendations |
| 1. Use of Multifactor authentication can reduce the chances of an attacker gaining access to a staff member’s account. Therefore, it prevents the chances of sensitive information to be leaked.  2. Use of token authentication is much more secure than the use of traditional passwords. Token authentication uses secure code that has already been authenticated. They are user specific, log-in session and the algorithm used. |
| Administrative Control Recommendations |
| *1. Ethics\_policy.docx*  *2. Acceptable\_use\_policy.docx* |