|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Information Sheet** | | | |
| Risk ID : 01 | Date: 4 Mar, 2020 | Prob: 80% | Impact: Very High |
| **Description:**  The recording of any human being can be used as input and output can be used as an evidence to any un-spoken words of that human being. | | | |
| **Refinement/ Context:**  Sub condition 1: If call recording is done by culprit and used as input to the software.  Sub condition 2: Telephone cloning by any hacker.  Sub condition 3: Software takes recorded files as input. | | | |
| **Mitigation/ monitoring:**   1. Software should not accept the prior recording as the input to the software. 2. The input should be only accepted from the microphone. 3. The output recording of cloned voice should contain encrypted knowledge of the user who has given input. | | | |
| **Management/ Contingency plan/ Trigger:**  Time span for the project is 3 months. The input from microphone can be made only option at first but, it can be modified later on in last month. The user for taking the input must be verified from the Google account or any authorized source. | | | |
| **Current status:**  4 Mar, 2020: Mitigation Steps Initiated. | | | |
| **Originator:** Gursimar | | **Assigned:** Sandeep | |