|  |  |
| --- | --- |
| **Risks** | **Preventative measures** |
| Release of user information: emails in particular | Use of secret keys and changed settings for database access. |
| Loss of user data due to physical damage | Storage performed off site using GCP services with provisioned locations and monitoring. |
| Malicious manipulation of data | User login required to create database entry and access protocols to prevent man in the middle interference.  Password hashing, secret key use and trusted ip monitoring.  Double login recognition. |