Cloud Management:

1. Following are the cloud platforms with their ownership in Data-Pilot. Junior team members cannot create or delete any resource without the approval of the cloud management lead:
    1. AWS (Irfan Umar)
    2. Azure (Aqeel Syed Shamsi)
    3. GCP (Sana)
    4. Cloud management leads will also inform beforehand the creation and usage of any instance to other relevant cloud management leads.
    5. **Ali Mojiz has the final approval.**
2. Server locations of the cloud platforms are as follows:
    1. AWS (1. Mumbai, 2. Singapore)
    2. Azure (Southeast Asia)
    3. GCP (Bilawal’s input is required)
3. We will decide the Nomenclature for the names of the cloud instances. Every team member must follow that Nomenclature. (*Action)
4. Cloud Management Leads have access to all the services of the cloud platforms. On the other hand, other team members have only access to their needful resources of the cloud platforms.
5. All Cloud management leads need to generate bill alerts for $3 per day.
6. The production environment will only be accessible by team leads.

Security:

1. All the credentials and access tokens will never be the part of code and should be stored in the secrets or environment variables.
2. Before uploading code to GitHub, or DevOps, please consult with your project leads every time. They will review the code and make sure of good coding practices and code security to avoid possible data breaches.
3. All the team members can use the Data-Pilot Gmail account (data.pilot1@gmail.com) for medium, colab, towardsdatascience, and GCP.
4. All the clients’ accounts access will be transferred to the 2nd Data-Pilot Gmail account (datapilottech9@gmail.com) and the following leads will have the access to the account other than Ali Mojiz: Irfan Umar, Aqeel Syed Shamsi, and Bilawal.
5. All the clients’ Facebook and Instagram access will be shifted to datapilottech9@gmail.com from personal accounts.
6. Service accounts for data warehouses and databases should have limited access to the team members. Mostly it should be read-only access for members other than team leads.
7. One-time secret service (https://onetimesecret.com) should be used against the team members in case they need ad-hoc access to the data.

8. All the documentation should be maintained on Notion.