* AS discussed during the Presentation – Sizing includes Logs of the system / Application / Database
  + - Logs generated is also considered in the storage Part like, Application, API, DB, Access Logs nearly more than 3 years.

             Infra Team is working on the system logs by moving them into the S3 bucket.

              For Application and Database please check with the relevant Team.

* Limitations in the Data Type should be defined (upload formats / sharing data formats like, Pdf, Jpeg etc.,)

Please check with the Client and Application Team.

* File / Attachment Size should be restricted to defined limit (like 500kB or 1 MB).

Please check with the Application Team.

* Data Retention Period should be Considered (Policy to be defined with Business Approval).
  + Retrieval of Data Access like attachment / Records from the Archived Data should be appropriately retrieved to the specific defined records / Leads.

Please check with the BA and Client for the Retention period.

**Note:** please update us, so that we will define the backup policy.

* As requested earlier, suggest the Endpoint Threat Protection software enablement in AWS to prevent Infections from Malware Protection as the data / attachment (like PAN, Aadhar, etc.,)may contains malware.
  + While attaching – content should be scanned before uploading the file.

Infra Team are working on the Endpoint Threat Protection software

* Visibility of Log Management should ease administrator to identify, Track, take action and remediate accordingly based on the events generated. (from system, application, DB covering API Management as well).

SysArc will suggest the API management software to tafe.

* Option to enable the movement of Logs to Centralised Log Management at On premise storage like, Application Access Logs (Activity Logs), Admin Logs, Application, Error / system critical Logs.

               Infra Team will check and update you.