BYOD Policy

- The main risks in this policy are

1. Devices are not being monitored by company
2. In case of theft/hacking company data is in risk
3. Friends/family of employee can access company data

- Each device needs to install a secure company software and needs to maintain a separate user account for company work
- Quick Heal Total Security is mandatory on all devices , All microsoft office apps are allowed , 3rd party apps like Zoom meetings , Trello are not allowed.
- Only AWS services can be used to store company data.
- Backup should be carried out using EaseUs Backup tool , Data should be backed up daily and it should be stored on company HDDs.
- Employes are only allowed to connect to their Home network or Office secure network.
- File sharing only through lms secure website and MD5 hash to be sent for integrity verification.
- While logged into the work account no personal messages/emails can be accessed by any employee.
- Chinese websites , Torrent websites and all Adult websites will be banned on these devices.
- Devices should not be given to friends/family with the company account logged in.

- Only the Finance and Human Resources team can bring their own devices to work.
- Only Laptops and Apple iPads are allowed to be used for company work.
- Company will have power to monitor the device 24*7 to verify that the data is safe and no intentional/unintentional data breach is taking place.
- An allowance of Rs. 5,000/- will be given to each employee per month for using personal devices.
- If any data breach is found it needs to be reported to the cyber security team via email and the cause will be investigated.
- The I.T team will be responsible for the training of employees for the usage of BYOD.