Data Storage Policy

- When data is stored on paper, it should be kept in a secure place where unauthorized people cannot access it
- These guidelines also apply to data that is usually stored electronically but has been printed out for some reason
- When not required, the paper or files should be kept in a locked drawer or filing cabinet (which has been labelled in advance) & that too in files / folders labelled as per company policy.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer. Data printouts should be shredded and disposed off securely
- When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts
- Data should be protected by AD passwords that are changed on a periodic basis and never shared between employees
- If data is stored on removable media, these should be kept locked away securely when not being used
- Data should only be stored on designated drives and servers
- Servers containing personal data should be sited in a secure location
- Data should be backed up frequently- the backups should be tested regularly, in line with the company’s standard backup procedures- i.e. either in authorized shared drives which can be accessed via company LAN or VPN or on One Drive
- All servers and computers containing data should be protected by approved security software and firewalls

ISMS Policy, Data Privacy – Ver 05, Doc No- MJ/ISMS/DP, Prep-Abhishek Kar