Important Notes and Best Practices.

- **To avoid virus attack** on the DSafe Destination/Server machine.
  - Do not share any file/folder/drive.
  - Do not access another machine from DSafe Destination/Server machine.
  - Only access via DSafe
  - Avoid Destinations, Directly Shared with End Points.
  - Do not download any harmful files/email attachments.
  - Use only for DSafe
  - Never use Pendrives etc.
  - If exposed to the WAN open only ports needed by DSafe
  - If exposed to WAN recommended to have an additional physical firewall layer.
- To ensure Backups are taking place at least one person in your organization should monitor the **backup logs on daily basis** and also keep a watch on the **Free Space on Destination Drive/s**. Monitoring can be done via email logs too.
- It is highly recommended to randomly restore your backups once a month to assure yourself of the **correctness of the backup**. It is important practice to detect media errors etc, at an early stage.
- It is recommended to have a **Disaster Recovery Destination** too if possible.
- **Before formatting a DSafe machine** you must uninstall DSafe. At that time you will be given an option to backup DSafe System data. This data is important for continuing your backups without refresh upon re-installation. After re-installation you may restore this DSafe System data via ‘Tools | Restore System Data’.
- To additionally safeguard the **DSafe System Setups** you will need it’s backup taken into another machine. Select it from ‘Setup | DSafe System Backup’. This is possible only if there is at least one DSafe Client installed apart from the DSafeServer. This is important because a fresh installation of **DSafeServer will not recognize the old DSafe Clients**.
- It is necessary to **keep the DSafe version updated** especially upon change of Minor Version.
- **Local Destination** is best option for speed and Security. In case there are remote machines you will need to make the **IP public**.
- Shared NAS is not recommended option for destination, this is kept for legacy support only. **NAS can be used efficiently with FTPS option**.
- Depending upon your Network speeds you must optimize ‘**Maximum Simultaneous Copy**’ so as to avoid Network Jams and at the same time allow multiple file transfers.
- You need to check **‘Default Excludes’** to know which files/patterns will be excluded from backups.
- Destination machines have to remain connected to the DSafe Server machine always. Client machines need to connect once in 10 days at least.
- For **Cloud Destinations being synced** with a Machine there is always a chance of User / Another Program deleting the DSafeBack Folder/Files. Necessary precaution has to be taken by you as same may get synced to the DSafe Backup on the Cloud.
- Check Network Status for WorkDrive & System Data Drive, change if necessary.
- Note that Microsoft Onedrive/ Sharepoint maximum single file size is 100GB.
- Onedrive/Sharepoint Upload should be completed within 24 hours per file, failing which resume option will expire.
- Onedrive/Sharepoint Needs Authentication every 90 days, kindly Re-Authenticate in DSafe too.