ANNEXURE – 1

General Guidelines to be followed regarding Cyber Security

1. Up to date Antivirus/ Windows Security should be installed in all the PCs/ laptops being maintained by respective offices.
2. Any incident related to cyber security e.g. Password hack, Ransomware attack or data corruption due to unknown reasons must be reported by respective ISOs to CISO@PSTCL.org.
3. Operating Systems of PCs/Laptops must be updated regularly with latest patches and upgrades.
4. Backup of important data stored in PCs/ Laptops must be taken on periodic basis (i.e. daily/weekly etc. as per office requirement & policy).
5. PCs/ Laptops/ email accounts password must be strong and should not to be shared with anyone by respective users. Also these passwords must be changed periodically for security reasons.
6. Only official email IDs should be used for official correspondence.
7. Pen drives/any other external media from unknown sources should not be used in official PCs/Laptops. Similarly, any external devices owned by PSTCL officers/official should not be used in the unknown PCs/Laptops.
8. Pirated software should not be used in official Desktops/ Laptops strictly.
9. Avoid downloading from freeware websites, websites of dubious nature, etc.
10. Don't click on attachments from unknown sources received in emails

EIC/ HIS&D-cum-CISO,
PSTCL, Patiala