

BEST PRACTICES TO BE FOLLOWED



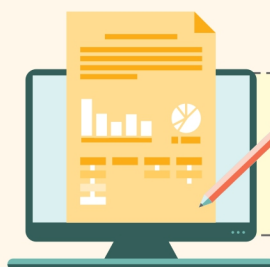
Deploying controls and policy for virtual, remote and physical access security



Using firewall and filtration and blocking websites and web content



Developing and practicing Business Continuity and Disaster recovery plan



Monitoring compliance to regulatory requirements



Encouraging reporting of incidents, threats and vulnerabilities



Arranging customized awareness and training programs for employees



Regular auditing systems and processes



Using encryption for sensitive data



Maintaining whitelist and blacklist of software, URL and applications



Scanning content/ attachments in email and storage for malware detection

