Annexure A
PSD Circular No. 03 of 2020

Additional Security Controls for Working from Home Scenarios

- Senior Managers to remain extra vigilant and guide resources diligently.
- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations.
- Ensure IT security personnel are prepared to ramp up the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery.
- Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications—such as rate limiting—to prioritize users that will require higher bandwidths.
- Connectivity to the internal organizational resources shall be properly protected through the usage of encrypted communication channel such as VPNs that may be protected through MFA (multifactor authentication) or strong authentication mechanism. Implement solution to limit VPN connectivity to only corporate-trusted devices.
- Ensure the hardening of endpoints being connected to the internal corporate network over the internet.
- Measures to mitigate emails that spoof the organization's domain such as Sender Policy Framework (SPF), DMARC and DKIM etc.
- Avoid simultaneous communication with public (internet) and organizational network. Whitelist allowed types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains. Whitelist allowed attachment types in emails.
- Block unapproved CD/DVD/USB storage media. Allow connectivity of corporate devices with trusted smartphones, tablets and Bluetooth/Wi-Fi/3G/4G devices.
- Limit the administrator accounts to staff who do not use these accounts for emails, video streaming and web browsing etc.
- Logging and monitoring of remote access shall be properly recorded and all systems from where remote access will be initiated shall have latest security updates of both OS & Antivirus.