Securing Remote Workspace During COVID-19

	Security Incident Monitoring	Remote Connectivity	Communication	Collaboration Tools	Physical Workspace	Mobile Device Security	Laptops
1	Monitoring new threats of COVID-19	Remote access policy must be created and circulated	Information security policy changes must be clearly communicated to all	Users must be trained on how to use collaboration tools safe and securely	Waste must be disposed and controlled in a well manner	MDM must be implemented to secure corporate data	Webcam cover protections should be provided to employees
2	Post-incident review of COVID-19	Pre-bandwith testing must be performed before starting the remote work firm-wide	Users must be provided with regular guidance on COVID-19 related cyber threats	Security controls must be implemented on collaboration tools such as patching, hardening, etc.	Clean desk policy must be enforced and reviewed	Mobile data backup must be taken on a periodic basis	Least privileged accounts should be implemented
3	Preparing IR plan of COVID-19	Role based access controls must be implemented for all level of users	Users must be provided with information on secure data handling	Logging and monitoring must be enabled for collaboration tools usage	Encourage employees to use hygiene products (masks, sanitizers, etc.)	User authentication must be enforced with a strong pin/pattern/password	Regular data backup must be taken from all laptops
4	A security team must be able to collect data from end-user system during remote working	Disable split tunneling via corporate VPN	Crisis management team and plan must be setup	Role-based access controls must be implemented for tools usage	First-aid kit and other necessary medical equipments must be present at the office (thermometer, cold-flu medicines, etc.)	External connections to the device must be restricted, such as USB, Hotspot, insecure Wi-Fi, Bluetooth, etc.	Laptop OS must be patched, hardened and account security controls must be implemented (CIS benchmark)
5	SOC team must be able to monitor cloud-based applications during remote working	A connection must be encrypted using high-end algorithms and protocols	Provide safe remote working training to employees	DLP must be implemented in order to protect data	A ventilation system must be properly working	Anti-theft measures must be in place for mobile devices	Drive encryption must be implemented
6	Incident reporting process and escalation matrix must be clear to all members who are participating in the IR process	Monitoring of logs must be enabled by SOC team		Data of the collaboration tools must be protected at REST and in MOTION	Enforce employee to stay home if they are feeling sick and encourage them to consult a doctor	Storage encryption on the devices must be enforced	VPN based remote access must be given to all employees
7		Two-factor authentication must be enabled		Usage of collaboration tools must be provided with a corporate VPN only	COVID-19 infection response plan must be communicated with users	Mobile device operating system must be updated to the latest	Restrictions must be put in place for removable media access
8				IAM must be implemented in order to access collaboration tools	Hygiene and awareness posters must be stuck on various walls	Security updates must be enforced on mobile devices	End-point security controls must be implemented on laptop devices
9						Anti-virus and anti-malware protection must be implemented	