Administrators Guide

Quick read checklist for Secure Remote Working

Sec-1 part of
claranet cyber security

Secure remote working

Cybersecurity checklist for remote working

- **Unsecured wifi networks**
- **Using secure devices for work**
- **Using home networks**
- **Phishing scams will target the remote workforce**

The ink on the corporate homeworking policy is probably still drying as we all prepare for a new working environment. New measures may already be in place to which we would absolutely recommend referring to this information. As always, if you are not sure you should ask as there could be specific recommendations in relation to how you work and what you access.

It is essential that you deploy some or all the following security measures:

- **A structured policy for remote working that adheres to the principle of least privilege to limit the access or functionality that different users have**
- **Least privilege principles must be extended to data and systems which may require a reconfiguration of any remote access solutions**
- **Deploy multi-factor authentication (MFA) for all remote access**
- **Encrypt client devices to protect stored communications and data**
- **Patch patch patch**
- **Endpoint security on desktops, laptops, smartphones and tablets is critical**
- **Risk Assessment should be carried out. A DPIA should also be carried out as there will be new risks to personal data being accessed and processed remotely.**

Your checklist should include the following:

Remote access	Decide how your remote access will be provided e.g. VPN (IPSec or SSLVPN), Direct Access, portal based (SSL VPN), or remote desktop access*. Ensure supporting infrastructure is adequate to handle the demand (I.e. internet bandwidth, license considerations). Consider removing the ability to provide split-tunnelling where remote access solutions are used. Split-tunnelling enables the connection so only traffic for corporate resources passes over the remote connection, while internet connectivity goes directly over the Internet, thereby bypassing any corporate security mechanisms. Unless there is a real business need or technical constraint to why split-tunnelling must be used, disabling the use of split-tunnelling would be the preferred configuration. All access whilst the user is connected to the remote access solution will traverse the corporate IT systems and be subject to any security controls imposed upon them. **Note: Remote desktop should be published securely to the Internet.*

Permitted devices	Ideally, access to corporate resources should only be accessible via trusted devices. Usually these devices are provided by your IT department and therefore the security of said devices should be known and trusted. This may prove problematic during the current COVID-19 crises, consider yhe use of Virtual Desktop Infrastructure (VDI) solutions which can give organisations some additional control (e.g Citrix, Terminal Services, AWS WorkSpaces) where less trusted devices need to be used.
Authentication	Strong authentication is critical to a remote access solution. The solution may not be protected from the untrusted public Internet using Firewalls and other security devices; therefore, it is important that the authentication mechanisms and remote access solutions are robust enough to protect against password bruteforce attempts. Multi-Factor Authentication should be deployed as a further defence against bruteforce attempts and to provide further assurance that the user authenticating is the intended user due to the MFA mechanism deployed.
Authorisation	Users should only be given access to systems and data that they have business need to access for that user to perform their job function. A properly configured and secure remote access solution should provide the user with the same access as if he/she was on the Internal network.
User access controls	It is important that the remote access solution can provide enough granularity to help restrict user access to data and systems. Incorrectly configured remote access solutions can give wider access to remote users either through misconfiguration or because of a lack of functionality within the solution.
Device encryption	Where permitted devices may come into contact with confidential information or personally identified information (PII), these devices MUST employ strong disk encryption to protect the data. This can prove to be problematic for BYOD, which may be less important where VDI solutions are deployed if these environments are configured to ensure information is not saved to the host machine.
Data storage	Organisations have a duty of care to protect corporate data, credit card data, and customer data, especially PII. The most effective way to achieve this is to limit access and limit storage locations of the data. By limiting storage locations, organisations can deploy security mechanisms and access control techniques to help protect data from unauthorised access, modification and deletion. As organisations start to

	extend storage locations, it becomes much more difficult to manage access and the security of the data. If technologies and mechanisms are not implemented to stop data being stored on devices being used for remote access, it becomes extremely difficult to provide adequate security controls and will cause issues for GDPR subject access requests as organisations will not have full visibility of where data is. . Look at restricting the flow of data based on users need to help restrict and control data storage.
Approved communications platforms and tooling	Remote working could see staff introduce their own systems instead of using those supplied by the company. Decide on a corporate strategy for approved software to be used by employees and make it easy to use. Use of tools like DropBox could mean corporate data or sensitive information is stored in places with no monitoring and lower security controls, in uncontrolled and unmanaged silos compromising data privacy and compliance, and in some cases can rack up significant costs.
Malware and Endpoint Security	Malware is on the rise; attackers are already manipulating fear associated with COVID-19 to exploit remote workers. Endpoint detection capabilities for Malware are essential, where possible you should deploy next generation malware protection such as SentinelOne as these have greater ability to detect new and unclassified attacks that traditional antivirus misses, plus they have the added benefit of isolation, remediation and rollback features to remove the need to pay a ransom!
Patching policy	Endpoints should be configured to contact the software vendors resources to gain product and security updates automatically. Centrally managed (not including cloud services such as Microsoft InTune) patch management tools are good to use however you should consider how frequently your users connect to the network to receive updates. If not frequently enough, endpoints could remain unpatched and become vulnerable to a breach.
Session locking	Ensure that remote devices are locked after an acceptable period (perhaps 15 minutes). To gain access, the user must be forced to reauthenticate.
Allowing access from unmanaged devices (BYOD)	Where users or third parties need to connect to the network, but the endpoint cannot be managed, consider deploying virtual desktop environments for remote connectivity. This image acts just like a full computer with an operating system and application software but provides corporate control for updates, security configuration and data security. Alternatives include AWS WorkSpaces.

	Additionally, many legacy Windows operating systems are now out of support so may become vulnerable. Ensure a minimum OS version is being used. XP and Windows 7 should no longer be permitted.
Always keep back-ups	What would happen if you lost your data? The cause can be varied from hardware failure to, application crashing, device theft. Users of Office 365 or other cloud-based productivity applications should always create and store their documents within the cloud platform, back up is automatic in these cloud platforms and disaster recovery in-built. If you're a OneDrive or GoogleDrive user, save your document to your locally syns'd folders to make sure it's saved in the cloud too (you need to be connected to the internet for this to work). Use external, encrypted hard drives if cloud options are not available.
Security monitoring	Capturing logs and analysing them for malicious activity such as malware or ransomware attacks or unauthorised login attempts is critical in the battle to prevent or contain a data breach. Ensure that logs are correlated, that alerts are responded to quickly and that regular reviews of activity take place.
Email and Web Content Filtering	Content filtering is the use of a program to screen and/or exclude access to web pages or email deemed objectionable. Content filtering is used by corporations as part of their firewalls, and by home computer owners. Content filtering works by specifying content patterns – such as text strings or objects within images – that, if matched, indicate undesirable content that is to be screened out. A content filter will then block access to this content before a user can click the link! This highlights why VPN split-tunnelling should not be used.
IT-Support	Users are going to need support, tokens may go missing, connections could be unstable. How will you ensure your workforce receives the support they need to remain productive? • IT Support – all things from locked accounts to faulty hardware. • Troubleshooting – use remote sessions and real-time monitoring to help • Provisioning desktops and devices – how much time is needed to onboard new staff. Use device images to speed up deployment. Ensure the organisation has a robust mechanism for validating an end user's identity BEFORE making any password resets or other account changes.

System administration	Ensure the availability of the remote access system by developing a policy and program of monitoring and maintenance keeping systems healthy, patched and operational.
User awareness	Remote workers must be provided with a basic level of security awareness to avoid become a victim of a phishing attack, to understand the risks of public Wi-Fi, and to ensure that home networks and properly configured. It's a good idea to have a checklist and regular reminders that the homework is now part of your perimeter defence and that there are simple actions that can be employed to limit risk.

Spread the word. Download the Quick read checklist to secure remote working for end users to share with your homeworking colleagues.

Contact us on 01924 284240 if you have any questions or would like to speak to a member of our security team.

Sec-1 part of

claranet cyber security

Visit: claranet.co.uk/services/cybersecurity