*Below are recommendations for technical controls that your organisation should consider in relation to remote working and as appropriate to your business operations and practices.*

*You can use the below to note down where your organisation is with deploying each type of control and log any other comments that might be relevant. For example, benefits to the business objectives and concerns related to the potential consequences of not putting a control in place could be noted, and would be a useful inclusion in any business case for investment in such measures, to the board or senior management.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Risk Control** | **Guidance** | **Status** | **Comments** |
| **Virtual Private Network (VPN) Access** | Where users are connecting via unsecured networks or using a device, PC or laptop that isn’t a company issued laptop dedicated to your organisations network, VPN is a critical control that should be employed as it encrypts data that is connected between the user’s pc or device and the organisation’s network.  |  |  |
| **Multi Factor Authentication (MFA)** | Being able to approve the identity of the person (or device) trying to gain access to your company’s network or systems should be a priority when defending against those trying to gain unauthorised access. It is important to implement controls that offer 2-factor or multiple layers of authentication – i.e. something you know (e.g. password); something you have (e.g. a security token); and something you are (e.g. a fingerprint). |  |  |
| **Using** **Up to Date Operating Systems** | Ensure that all computers and devices being used to access work systems are operating on up-to-date supported operating systems.For example, as of January 2020, Windows7 is no longer supported, and computers using this operating system are more prone to cyber attack.   |  |  |
| **Network Encryption** | Information in transit should be appropriately encrypted. Some protocols that could be deployed include [*Using IPsec to Protect Data*](https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data)*and*[*Using TLS to protect data*](https://www.ncsc.gov.uk/guidance/tls-external-facing-services)*. (NCSC).* Staff should be educated on utilising the protocols with a clear policy and guidelines that can always be referenced easily. |  |  |
| **Cloud Based Services** | Cloud software solutions are becoming popular and recommended to reduce risk as data in the cloud is encrypted and access can be controlled by your security team/management. Use secure cloud-based solutions and educate staff to save data on these rather than on devices such as laptops/mobiles which can be easily compromised. If cloud storage is not available to your organisation or staff, central drives should be available for saving sensitive information, and staff must be cognizant never to save documents to local folders / the desktop. |  |  |
| **Firewalls** | These are critical gatekeepers for your organisation’s networks and remote devices, working on a set of rules that monitor and protect inbound and outbound data. Software firewalls can be deployed on devices via a program. Physical firewall devices are generally deployed at the perimeter of each network access point. |  |  |
| **Technical Risk Control** | **Guidance** | **Status** | **Comments** |
| **Anti-Malware Protection** | This is a primary method of defence as malicious software (malware) is involved in most cybercrimes. It is crucial that up to date ‘NextGen’ anti-malware is employed across all devices that carry, store or transact information. Traditional and old forms of anti-malware or anti-virus software is no longer enough to defeat the significant increase in evolving malware that is introduced each day. |  |  |
| **Data Loss Prevention** | Technologies can be implemented, or devices can be adapted to offer technical security against data loss, e.g. disabling USB ports on laptops and devices. If such technologies are not possible, then procedural controls will need to be enforced for staff to follow – e.g. bans on using removable devices. |  |  |
| **Mobile Device Management (MDM)** | A useful tool for security response teams / IT to have access to, in order to minimise the impact of any compromised device. MDM can control the operation of mobile devices remotely and wipe information or disable access to them, For example, for a device that has been reported lost or stolen.  |  |  |
| **Network Monitoring / Intrusion Detection & Prevention Software** | Appropriate technologies should be identified for your organisation to enable proactive monitoring of communications and unwanted information that passes through all devices connected to the organisation, offering timely alerts in order to prevent or minimise the impact of any breach. Some programs can also block and remove unwanted intrusions.  |  |  |
| **Endpoint Detection & Response Solutions** | Enables IT teams to view all endpoints to remotely prevent malware, deploy patches, and perform other activities automatically. Such a technology is generally powered by artificial intelligence/machine learning and offers continuous monitoring and response to mitigate cyber threats.  |  |  |
| **Back Up Solutions** | Effective investment in such a facility for critical and sensitive information can be invaluable in situations such as when faced with a ransomware attack. Organisations should never pay a ransom and if appropriate backups, which are refreshed on an appropriately regular basis are in place, minimal impact should be encountered, and focus can be placed on securing all vulnerable access points to mitigate against future attacks. |  |  |
| **Security Settings** | Ensure all security settings are set to **HIGH** for devices used for activities related to the organisation. |  |  |
|  |  |  |  |

*Appropriate research should be undertaken to understand and identify the most effective technical solutions for your organisation, as for each of the defence methods there are often many options available. Ensure you consider your organisation’s current and future potential remote working practices when selecting risk management solutions.*

*Technical security controls should be reviewed regularly and updated to meet the organisation’s current threatscape. At minimum, an annual security risk and controls review for your organisation is recommended.*