National Security Inspectorate
Sentinel House, 5 Reform Road, Maidenhead, SL6 8BY
E: nsi@nsi.org.uk | W: nsi.org.uk

Requirements for use of a Virtual Office Environment

1 Cyber security assessments

Hold and maintain Cyber Essentials, with records retained for audit purposes. This certification should be renewed biannually.

2 Secure network connection

Employees must ensure they have a secure Internet connection at their workspace, preferably a wired connection or alternatively a Wi-Fi connection using WPA2 encryption or higher.

Access to public Wi-Fi networks should be discouraged for work-related activities and may only be used for limited periods and when protected using a company-approved VPN.

3 Use of VPN (Virtual Private Network)

Employees should use a company-approved VPN to securely access company resources and data.

VPN software must be kept up to date with the latest version and all security patches applied.

4 Strong authentication mechanisms

Multi-Factor Authentication (MFA) must be enforced for accessing company systems and applications.

Passwords must adhere to a strong password policy, including regular updates. They must be subject to change every 12 weeks and must be 8 digits made up of alphanumeric parts.

5 Endpoint security

All devices used for work (laptops, desktops, mobile devices) must have up-to-date antivirus and anti-malware software installed.

Updates for operating systems and applications must be enabled. Either using automated updates or as part of an organisations wider IT policies.

6 Data encryption

Data stored on devices or transmitted over networks must be encrypted, especially sensitive or confidential information.

We recommend the use of encrypted communication channels (such as encrypted email or messaging apps) when sharing sensitive data.

7 Secure file storage and sharing

Company-approved cloud storage solutions should be used for storing and sharing files securely.

Employees must not use personal cloud storage, file-sharing services, or personal physical storage media (IE USB sticks) for work-related data.

All paper copies of confidential documentation must be securely managed and stored before being uploaded to secure cloud storage, adhering to established protocols for document handling and protection with evidence of a secure disposal process available for audit.

No company-related documentation is to be left in vehicles.

8 Remote access policies

Clear policies should be established and documented for remote access to company systems and data.

Access permissions should be granted based on the principle of least privilege, ensuring employees only have access to the resources necessary to carry out their roles.

9 Regular security awareness training

Employees should undergo annual training on cybersecurity best practices, including phishing awareness and social engineering tactics, evidence of this should be retained. This can be done by online learning.

10 Physical security measures

Employees must ensure the physical security of their work devices, such as locking screens when not in use and storing devices in secure locations when not in use.

11 Incident response plan

Develop and regularly review an incident response plan outlining procedures for responding to cybersecurity incidents, including reporting procedures and escalation paths.

12 Compliance with regulations

Ensure compliance with relevant data protection regulations and legislation (e.g., UK GDPR & Data Protection Act) and any industry standards.

Note: This should also cover the staff work environment and the risk of private client-related calls and emails/systems being observed by unauthorised persons.

13 Availability of welfare

During the audit or any other NSI meetings, a secure dedicated private space must be provided by the company. This space must also have access to welfare facilities such as a toilet and drink-making facilities.