Remote Access Policy

TechTonic Shift

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Amendment | Author |
| 1.0 | 04/11/2024 | New Policy | SR |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Remote Access Policy for Clients**

**Introduction**

This policy outlines the procedures for remote access to your systems by TechTonic Shift technicians. Remote access allows our technicians to provide timely and efficient support, but it’s essential to ensure the security of your systems.

**Remote Access Tools**

To facilitate remote support, we primarily use TeamViewer and ScreenConnect. However, we are open to using other approved remote access tools at your discretion. Please note that using alternative tools may affect our ability to provide support and may introduce additional security risks.

**Security Considerations**

* **Strong Passwords:** Ensure that you use strong, unique passwords for all your accounts, including remote access tools.
* **Software Updates:** Keep your operating systems and software up-to-date with the latest security patches.
* **Phishing Awareness:** Be cautious of suspicious emails and avoid clicking on links or downloading attachments from unknown sources.
* **Session Monitoring:** Monitor remote access sessions to ensure unauthorized access doesn't occur.
* **Session Termination:** Terminate remote access sessions when they are no longer needed.

**Your Responsibility**

You are responsible for the security of your systems and data. This includes:

* **Choosing Remote Access Tools:** While we recommend TeamViewer and ScreenConnect, you may choose other approved tools.
* **Security Practices:** Adhering to best practices for remote access, including strong passwords and software updates.
* **Incident Reporting:** Promptly reporting any suspicious activity or security incidents.

**TechTonic Shift’s Commitment to Security**

We are committed to protecting your data and systems. Our technicians will:

* **Adhere to Strict Security Protocols:** Follow strict guidelines to safeguard your information.
* **Use Strong Authentication:** Employ strong authentication methods to access your systems.
* **Limit Access:** Restrict access to authorized personnel only.
* **Regular Security Training:** Undergo regular security training to stay updated on the latest threats and best practices.

**Disclaimer**

While we strive to provide secure remote access, we cannot guarantee complete security. Using alternative remote access tools or neglecting security best practices may increase the risk of unauthorized access or data breaches. You assume full responsibility for the security of your systems and data when using alternative remote access tools.

By agreeing to this policy, you acknowledge and accept these terms. Please contact us if you have any questions or concerns.