Remote Access Policy

1.0 What's the point of a Remote Access Policy?

So, you're at home wearing a very professional shirt. Looking good! But you're also wearing pajama bottoms and elf socks that light up when you wiggle your toes. Sigh. Anyway, you need to sign into our organization. To keep everything secure and protected when you're working remotely, we need a policy for signing into our systems and networks. (But you should know that we're deeply disturbed about your socks, and we wish this policy could address them.)

- ❑ Remote access allows authorized individuals to connect to our systems from outside our physical premises, even if they are wearing ridiculous things on their feet.
- ❑ As always, this is about the safety and success of our organization, so by using this policy, we aim to ensure the security and integrity of our systems while enabling convenient and secure remote access for our employees and authorized parties.

2.0 Who needs to know about this Remote Access Policy to stay out of trouble?

YOU! That's right. You! The person sitting there wiggling your toes!

- ❑ This policy applies to everyone: all employees, contractors, and any other individuals granted remote access privileges to our organization's systems and networks.
- ❑ It covers all remote access methods, including but not limited to virtual private network (VPN), secure shell (SSH), and remote desktop protocol (RDP). It is our responsibility to ensure compliance with this policy, and failure to do so may result in the revocation of remote access privileges.

3.0 At No Extra Cost: $20 Words

Since you and your socks seem to imply that you aren't up on the latest definition of "style", we want to define a few terms related to this policy for you. You know, just to be clear. (And stop wiggling your toes. It's distracting!)

- ❑ Remote Access: The ability to connect to our organization's systems and networks from a remote location. In other words, you're there. We're here. We connect. It's all good!

- ❑ Authorized Individuals: You need permission! So, only employees, contractors, and other individuals who have been granted explicit permission by our organization to access our systems remotely are allowed onto our network.
- ❑ VPN (Virtual Private Network): This is a secure encrypted connection that allows remote users to access our internal network securely over the internet. Think of it like a secret code for our private club.
- ❑ SSH (Secure Shell): We want to keep our documents safe during a file transfer so, this is a cryptographic network protocol used for secure remote access and secure file transfers over an unsecured network. This is all about protecting files that we share.
- ❑ RDP (Remote Desktop Protocol): For all of this to work, we'll need something that enables users to remotely access and control a computer over the network. We only use Remote Desktop Protocol from Microsoft when we can secure it with another form private network that prevents snoopers from seeing that this access method is available. If there's no way to lock it down, we shut it off! And that is how the magic happens – BOOM!
- ❑ Secure Access Service Edge (SASE): Actually, if you really want to hear about magic, this is it! SASE protects access to our information resources by combining network security and wide area networking (WAN) capabilities into a single cloud-based service. Very exciting! But wait! There's more. It includes features like secure web gateways, firewall-as-a-service, zero-trust network access, data loss prevention, and more. SASE solutions are our preferred method of securing remote access and will be used to secure network communication whenever and wherever possible.

4.0 Tell me more about the policy guidelines!

Okay! Here's the exciting part of this policy: THE GUIDELINES!! We know what you're thinking: Where have these been all my life? So, feel free to print them, and take them to an engraving store to get them carved into a steak knife or trophy. Your choice! So, in the next few sections, we're going to talk about the approval process, secure authentication, encryption, secure connection, endpoint security, monitoring and logging, and third-party vulnerability scans.

4.1 So, let's start with the approval process

Remember when you used the Magic 8 ball to figure out if your mom would let you spend the night at a friend's house? No? Well, we do, and it wasn't pretty. But here's the thing. You don't need to ask the Magic 8 ball (look it up if you don't know what this is) to get permission to use a remote access. Just ask the proper department.

- While we'd love to throw a party with cake and give you the keys to the kingdom when you do ask the proper department for permission; however, access will be granted based on the principle of least privilege. So, you'll get what you need to perform your duties, but nothing more. That keeps us all safe.
- But much like asking your mom if you could spend the night at a friend's house, requests will be reviewed and approved by the designated authority before access is granted.

4.2 Secure Authentication is the cat's pajamas

It's probably best if you never put pajamas on cats, but this used to be a phrase people said before the word "cool" was invented. Anyway, we all love having a secure, safe network, because this means good things for our organization. So, to keep everything right with the universe, remote access must be authenticated using strong, unique credentials for each user. Not to alarm you, but when things aren't right with the universe, there's the whole Darth Vader thing, and a ton of sequels. You get the idea.

- Yes, we said Darth Vader, which means we definitely want to use multi-factor authentication (MFA) whenever possible to provide an additional layer of security. Just keeping the dark side away… that's all we're saying.

4.3 Did you say encryption?

This is one of our favorite things to talk about, so we're glad you asked. All remote access sessions must use strong encryption protocols, such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL), to protect the confidentiality and integrity of data transmitted

over the network. What does that mean? Well, it's like that secret language you and your colleagues developed so you could talk about supervillains during the workday without your manager knowing… only better because your manager cracked the code on Day 1.

4.4 Don't you just love a secure connection?

Sure, "secure connection" sounds like a terrific title for a Romcom, but here we're talking about using secure and approved methods for connecting to our internet. So, please use things like VPN, SSH, or RDP.

- Don't you love getting new toys? Well, when we get remote access tools they come with default or well-known credentials. So, we want you to change these passwords right after you begin using them to prevent unauthorized access.

4.5 Please, can we talk about endpoint security?

Okay, so if you're connecting remotely, make sure that your device has up-to-date antivirus software and security patches. In other words, keep your device protected so that when you connect to us, we're all safe.

- Devices must be protected by a password or PIN and configured to lock after a period of inactivity.

4.6.0 Monitoring and Logging, the new dynamic duo

We're going to keep watch of remote access sessions, which means they will be monitored and logged, so we can spot any unauthorized access attempts or suspicious activities.

- Logs will be reviewed periodically to find potential security incidents or policy violations.

4.7 Third-party vulnerability Scans? Yes, please!

It's always great to have a helping hand, right? So, sometimes we may use third-party vulnerability scans to make sure everything is safe and secure.

- ❑ These scans will involve someone on the outside checking to see if we have any weaknesses within our infrastructure.
- ❑ The purpose of these scans is to take action before a problem emerges and reduce the potential risk to our systems and network.

5.0 Final Thoughts

So, what's the big deal? Well, we want you to be able to work remotely, but yet keep our systems and networks safe. This policy helps us do that. Cool, right?

- ❑ Obviously, it's really important for everyone to understand and follow this policy to safeguard our valuable resources and protect against potential security threats.
- ❑ Any concerns or questions about remote access should be directed to the proper department or designated authority.
- ❑ Together, we can keep a secure and efficient remote access environment.