**Remote Access Policy:**

**Document History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Summary of Changes** |
| **1.0** | **10/01/2023** | **Document creation and  approval** |

**Review Distribution**

|  |  |
| --- | --- |
| **Name** | **Job Title** |
| **Sabrina Senat** | **CEO** |
| **Paul Evans** | **President** |
| **Sally McCarty** | **Vice-President** |
| **William Clay** | **IT Team Supervisor** |
| **Tony Roch** | **Printing Manager** |
| **Jack Johns** | **HR Manager** |
| **Maria Garcia** | **Financial Manager** |

**Document Approval**

|  |  |  |
| --- | --- | --- |
| **Version** | **Organisation** | **Position Date** |
| **1.0** | **IT Team** |  |

**Objective:** The objective of this policy is to establish guidelines for the secure use of remote access technologies by employees, contractors, and other authorised individuals within ABC Technologies.

**Scope:** This policy applies to all employees, contractors, and other authorised individuals who use remote access technologies to access ABC Technologies network and resources. This includes, but is not limited to, the use of virtual private network (VPN) connections, remote desktop protocols (RDP), and remote access software.

**Introduction:**

A remote access policy is a set of guidelines that dictate how and when employees can access company resources remotely. This policy is designed to ensure that remote access is secure, authorised, and in compliance with the company's security standards. It also outlines the procedures that employees should follow when accessing company resources remotely, as well as any restrictions or limitations that apply (ISO, 2013).

**Principles:**

1. General access to the Internet from home through ABC Technologies network is permitted. If the user wanted to use the Intranet for recreational purposes the remote access connection must be disconnected prior to accessing such Internet sites.
2. All devices used for remote access with ABC Technologies must have the latest Windows operating system and is the employees responsibility to ensure all relevant updates are completed before establishing connection with the ABC Technologies network. This is a must as security issues need to be avoided.
3. Secure remote access policies will be in place when employees try and use the service. The employee will need to use a password their own username and passwords to login and will be used as identification – This will be the same as in office. Passwords will need to have the following to be accepted:

* A mixture of lower case and upper case letters,
* At least two number
* At least one extended character like “!”

Passwords must not be disclosed to anyone including family members when working from home.

1. Any remote computer equipment and devices used to connect to ABC Technologies must be owned by ABC Technologies and must have up to date antivirus software installed on them.
2. Any user using a public network to establish a remote connection with ABC technologies must use the VPN client provided by the remote access company.
3. Users who use WIFI must disconnect the wireless sessions when not in use to mitigate attacks from hackers or eavesdroppers.
4. Technical support cannot be provided for any WIFI related issues for public or home broadband from the IT services.
5. IT services must have the ability to reset passwords when the user requests.
6. The remote access privileges must not be or attempted to be changed by any employee approval from IT services.
7. The ABC Technologies Intranet system must not be used by any employee for the purpose of harassment, obscene behaviour, competitor interests and illegal transactions.
8. Timeouts will be used when remote access connections have been inactive for 15 minutes and terminate after 1 hour. The user is required to reconnect and reauthenticate for both time outs in order to reconnect to ABC Technologies network. If the remote access users account be inactive for 60 days the users privileges will be suspended and until IT services are notified, reactivating the account.
9. If ABC Technologies computer or equipment used for remote access is lost, damaged or stolen, the user who has the computer or equipment is responsible for notifying there manager and IT service immediately.
10. The users of the remote access agrees to reporting immediately to their manager and ABC Technologies IT services for any unauthorised access incidents or suspected incidents. Unauthorised disclosure of companies databases, networks, resources etc must also be reported.
11. Users of the remote access agree and accepts that the network connect to ABC Technologies is monitored to record duration of access, dates, times, etc. This is done to identify suspicious activity and unusual usage patterns, like with all in house computers.

(Williams, 2016)

**Disciplinary Consequences:**

* Any suspected or actual breach of this policy needs to be reported to vice-president, president or CEO of ABC Technologies through a suitable channel. Appropriate action must then be taken by the vice president, president or CEO where they will take appropriate action and involve any relevant external and internal authorities.
* Compliance of this policy must be followed else disciplinary action will be taken in accordance with relevant process.

(Buckinghamshire New University, 2015).

**Responsibilities:**

**IT team responsibilities:**

* Establish guidelines for the use of remote access and clearly communicating them to employees.
* Provide assistance, such as a helpdesk, to employees who encounter issues with remote access.
* Ensure that remote access to ABC Technologies network and systems is secure and that only authorised individuals are able to access them.
* Provide training and resources to employees to help them understand the importance of secure remote access and how to use ABC Technologies remote access tools.
* Regularly monitoring remote access activity and identifying and addressing any security incidents or violations of the policy.
* Keep records of any remote access activity, including login attempts and user access, to aid in incident response and investigations.
* Prevent any misuse of passwords where they are left out or given to someone else enabling an unauthorised user to access ABC Technologies network.

(Calder & Watkins, 2010)

**Third-party Data Processors**

* Regularly reviewing and updating the remote access policy to ensure it remains effective and relevant.
* Regularly monitoring remote access activity and identifying and addressing any security incidents or violations of the policy.
* Ensure that remote access to ABC Technologies network and systems is secure and that only authorised individuals are able to access them.
* Implement technical controls such as firewalls, virtual private networks (VPNs), and two-factor authentication to secure remote connections.

**Training and audit:**

* Keep records of any remote access activity, including login attempts and user access, to aid in incident response and investigations.
* Keep records of who and when undertook training and their scores to show how many attempts and questions were answered correctly.

(Watkins & Calder, 2019)

**Key Outcomes:**

* Enhanced security and protection of company resources: Implementing appropriate safeguards and controls, ABC Technologies can help to prevent unauthorised access or misuse of its systems and data, which can protect the security and integrity of its resources.
* Improved productivity and flexibility for employees: Enabling authorised employees to access company resources remotely, a company can help to improve their productivity and flexibility, as they are able to work from anywhere with an internet connection.
* Enhanced compliance with relevant laws and regulations: The remote access policy can help ABC Technologies to ensure that it is in compliance with any relevant laws and regulations, such as data protection and privacy laws.
* Greater transparency and accountability in the use of company resources: Remote access policy can help to ensure that employees are using company resources in a responsible and accountable manner, which can improve trust and confidence among stakeholders.
* Improved reputation and image: If ABC Technologies is seen as a responsible and trustworthy steward of its resources is likely to have a more positive reputation and image in the eyes of its stakeholders.

(Calder, 2017)

**Related policies:**

* **Acceptable use policy**: This policy outlines the acceptable and unacceptable uses of company resources, including guidelines for using company-owned devices and networks.
* **Password policy**: This policy outlines the requirements for creating and using secure passwords, as well as procedures for changing or resetting passwords.
* **Device security policy**: This policy outlines the measures that a company will take to protect its devices from unauthorised access or misuse, such as installing antivirus software and configuring firewalls.
* **Network security policy**: This policy outlines the measures that a company will take to protect its networks from unauthorised access or misuse, such as implementing VPNs and firewalls.
* **Encryption policy**: This policy outlines the requirements for encrypting data and communications when accessing company resources remotely, in order to protect sensitive information from unauthorised access or interception.
* **Website terms of use**: This policy outlines the terms and conditions for using a company's website, including guidelines for accessing and using the site and any resources or services that it offers. This policy may also include provisions related to the collection and use of personal data through the website.

(ISO, 2013)