Insert the organization logo by clicking on the image icon

Remote Access Policy Template

Date:

**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Title:** | Remote Access Policy Template | | |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  | |
| **Publish Date:** |  | | |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Objective 4](#_Toc97460088)

[2. Scope 4](#_Toc97460089)

[3. Policy 4](#_Toc97460090)

[3.1 General Requirements 4](#_Toc97460091)

[3.2 Remote Access User Responsibility 5](#_Toc97460092)

[3.3 Remote Access Devices 5](#_Toc97460093)

[3.4 Communication 5](#_Toc97460094)

[3.5 Encryption 6](#_Toc97460095)

[3.6 Third-party Responsibilities 6](#_Toc97460098)

[4. Policy Enforcement 6](#_Toc97460099)

1. Objective

In this day’s number of request for working out of office are increased and become a mandatory to obtain a Remote Access service for <entity name> employees, contractors, third-parties and stockholders to reach internal information’s and data external unsecured network (e.g. home, wireless, public, etc.), this policy is to minimize risks associated with using remote access service, and defines controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

1. Scope

This policy applies to employees, contracted personnel and any third parties representatives who have been provided to access remotely to organization/ entities internal network.

1. Policy

## General Requirements

1. Remote access compliance and procedure must be identified by the Designated Security Team (DST).
2. remote access requests shall be through the <entity name> requests process for management approval and must be conducted before network access granted.
3. Accessing internet must be routed through the <entity name> internet gateway during the remote access.
4. Remote access for individual services shall be secured such as deploying for a Hypertext Transfer Protocol Secure (HTTPS) to access web services (e.g. webmail, etc).
5. Long period granted remotely sessions shall be reauthenticated periodically after an idle time set by the DST.
6. Remote access employees must be authenticated by leveraging the AAA infrastructure established by the <entity name>.
7. Multi-Factor Authentication (MFA) must be implemented to all <entity name> employees before access granted.
8. DST must ensure all remote access are comply with <entity name> security policy before network access granted by implementing a Network Access Control (NAC).
9. Remote access to <entity name> information or data should be in accordance with Access Control and physical Security Policy.
10. All <entity name> employees must be aware of remote access compliance and procedure.

## Remote Access User Responsibility

1. Employees are responsible to ensure of their used devices to access <entity name> network are comply with remote access policy.
2. Employees are responsible to ensure of their network connection used to reach the <entity name> network are secured and not to connect to unsecured network, wireless access or public network.

## Remote Access Devices

1. All devices used for remote access must be up to date from devices OS, security patches, anti-viruses, anti-malware and host firewall.
2. Disable networking features such as Bluetooth, Near Field Communication (NFC), network pairing, tethering and hotspot during remote access.
3. Portable media and external storages must be prohibited unless when they are needed.
4. <entity name> information and data stored in remote access devices must be encrypted, backup and able to wipe in lost or theft.
5. Remote access devices must be protected physical by not been left unattended.
6. Bring Your Own Device (BYOD) shall not be used for remote access, however if <entity name> intends to use, approval from management is required before access granted to internal network and a certain level of security from the OS version, batches and updates based on DST instructions.
7. All devices used for remote access shall be in accordance with Mobile Devices Policy.

## Communication

1. Home wired network used for remote access must be secured by:
   * Changing the default password of the home wired devices.
   * Prevent administrated access to home wired devices from outside.
   * Configure the devices to silently ignore unsolicited requests.
   * Home wired devices must be check for updates and patches.
2. Wireless network used for remote access must be secured by:
   * Using strong authentication WPA or WPA2 certifications keys.
   * Using strong encryption AES 128-bit.
   * Permit access for remote devices by Media Access Control (MAC) address.
   * Changing for SSID name and hide it.
   * Disable administered access through the wireless network.
3. <entity name> agreed with Internet Service Provider (ISP) to provide for a dongle or MIFI for all remote access and must be secured by:
   1. Using for static public IP address for dongle or MIFI to add it in the <entity name> allowed access list.

## Encryption

1. Network connection must be secured and encrypted at transit by implementing:
2. Virtual Private Network (VPN) to initiate for a secured tunnel between the remote devices and the <entity name> security gateways.
3. Secure Sockets Layer Virtual Private Network (SSL-VPN) to provide access through standard web browsers or installing agent in the remote devices.
4. Remote System Control by providing the employees an access to secured virtual desktop with required privilege access to <entity name> network.

## Third-party Responsibilities

1. Remote access for third-party, contractors, business partners and vendors must be approved by the DST.
2. Signed agreement must contain the purpose of the remote access, time period, network and services privilege access required, revocation of access at the end of the agreement.
3. Provided remote access for third-party must be reviewed and monitor.
4. Misuse of the remote access must be revoked, reported and action must be taken based on the agreement penalty clause.
5. Policy Enforcement
6. Policy document sponsor and owner: <Head of Cyber Security Department>.
7. Policy implementation and enforcement: <Department Concerned with Information Technology>.
8. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-