SystemsSupportCorp
WE'RE LOOKING OUT FOR YOU

462 Plain Street Suite 206 Marshfield, MA 02050 (781) 837-0069

Remote Work Policy Template

Edit the policy to fit your situation as required. As always, the policy should be reviewed by a lawyer to ensure it conforms with local or federal laws.

Systems Support
IT Support & Service Since 1989

www.systemsupport.com

Email: info@systemsupport.com

SystemsSupportCorp
WE'RE LOOKING OUT FOR YOU

462 Plain Street Suite 206 Marshfield, MA 02050 (781) 837-0069

Remote Work Policy

Purpose

The purpose of this policy is to address vulnerabilities associated with staff working remotely. The goal of this policy is to provide a safe and functional work environment that will allow staff to work remotely. A focus of concern with remote work is staff-owned devices (laptops, PCs, smartphones, etc.) entering the company network, as these devices may not have the same controls as company-owned devices, and if compromised, could infect our network.

Scope

This policy covers all Company name's employees who have remote work capabilities.

Statement of Policy

Company name will implement, to the fullest extent possible, all necessary security controls to ensure staff can remotely work in a safe and functional environment.

Technology and procedure requirements for remote work

- Transmission security and integrity
    - Company name has ensured our firewall is capable of VPN traffic and that employees working remotely from corporate laptops or computers are provided with VPN licenses
    - Company name has ensured staff needing to use personal computers can securely remote connect to their work computer and operate as if sitting at your desk, utilizing software provided by {IT Support Company Name}
    - Company name has tested Unified Communication strategy and technology necessary for remote work: VOIP phones, softphone technology that transfers to mobile phones from the office number, and employees' use of internal chat technology and video conferencing.
    - Data sharing through external cloud applications (OneDrive, etc.) is restricted to only company approved and controlled applications
    - Staff can securely exchange files and information externally and internally *(i.e., email encryption option enabled, on-premises solution, enterprise class encrypted file sharing software etc.)*
    - Multifactor Authentication will be implemented for remote connectivity
    - Ensure remote connectivity sessions are set to expire after 4-8 hours
- Device and media controls for remote work

462 Plain Street Suite 206 Marshfield, MA 02050 (781) 837-0069

- Devices used to connect remotely (laptops and PCs) will utilize encryption
- These devices should not have admin privileges. If they do, then strong passwords must be used
- Mobile Device Management software will be implemented on all devices
- A Bring Your Own Device (BYOD) policy will be developed to define proper security for personal devices
- Remote endpoint security tools that can be centrally reviewed and monitored for company and employee-owned devices will be reviewed and implemented
- Access to Sensitive Company Information, Personally Identifiable Information (PII) will be restricted/limited when an employee is not using a secure workspace or device

- Incident Response procedures will include response to incidents originating from or affecting employees working remotely
- Remote workers will be trained on common social engineering and phishing scams

Controls for remote work environment

- Secure workspace
  - Remote work staff must have the ability to lock laptops, devices, and any business relevant information (i.e., paper documents) when not in use. Laptops and devices should be stored out of sight and/or in the trunk if it must be left in a vehicle unattended. Any other business relevant information (i.e., paper documents with sensitive information) should be stored securely
  - Remote work staff should be aware of their environment and who is around them. Safely perform conversations without visitors eavesdropping or shoulder surfing. Use screen protectors when necessary
  - Restrict the use of devices containing business-relevant information. Employees will not let family members, friends, or anyone but themselves use company-owned devices or personal devices used for business purposes
- Remote network security (Home Network)
  - Wireless security
    - Always change default Wi-Fi Router passwords
    - Enable WPA-2 or higher encryption
    - Ensure your local router firmware is up to date

462 Plain Street Suite 206 Marshfield, MA 02050 (781) 837-0069

    - The use of public Wi-Fi should be limited. Always use a VPN when connecting to public Wi-Fi. Never use public Wi-Fi to send sensitive information without a VPN
  - Ensure all personal devices are secure with company-provided or personally owned antivirus and antimalware software
  - Update IOT Device firmware (smart thermostats, surveillance cameras, doorbell cameras etc.)
    - Ensure default passwords are changed
  - Update software on all devices within your home network (Corporate laptop, IOT devices such as cameras and smart thermostats, personal laptops/tablets, etc.)
  - Review and follow corporate Bring Your Own Device (BYOD) and other relevant policies and procedures
- Remote Work Employee Awareness
  - Be extremely cautious of email phishing scams
  - Limit social media use
    - Don't reveal business itineraries, corporate info, daily routines, etc.
- Confidential Information/Personally Identifiable Information
  - Never send such information by email unless it is encrypted
  - Never initiate a transfer of such information because of a received email. ALWAYS confirm by phone or in person that the request was legitimate
- Financial Transactions
  - Never initiate the transfer of funds, be it Gift Card or other financial cards OR wire transfers without first confirming the legitimacy of the request by asking the person that originated the request either by phone or in person. If the person is unknown to you, contact your supervisor for direction.