L.A. CREATIVE TECHNOLOGIES
TOOLS FOR GROWTH

WORK FROM HOME 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 your network, as these devices may not have the same controls as company-owned devices, and if compromised, could infect your data network.

Scope

This policy covers all *<Company name>* 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.

Transmission security and integrity

- *<Company name>* has ensured that remote access solutions are available.
- *<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 & video.
- Data sharing through cloud applications is restricted to company approved apps.
- Staff can securely exchange files and information externally and internally.
- Multifactor Authentication will be implemented for remote connectivity.
- Ensure remote connectivity sessions are set to expire after 4-8 hours.
- 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

Device and media controls for remote work

- 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.
- 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), and electronic Protected Health Information (ePHI) will be restricted/limited when an employee is not using a secure workspace or device.

L.A. CREATIVE TECHNOLOGIES
TOOLS FOR GROWTH

WORK FROM HOME POLICY

Enviroment Control

Remote network security

- Wireless security.
  - › Always change default Wi-Fi Router passwords.
  - › Enable WPA-2 or higher encryption.
  - › Ensure your local router firmware is up to date.
  - › 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, 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.

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. Cable locks for laptops should be used when necessary. Laptops and devices should be locked 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.

CONTACT 323-454-1312 · inquiries@lacreativetech.com
ADDRESS 2206 Beverly Blvd, Suite #101 - Los Angeles, CA 90057