Organizational Function Area:	Information Technology
Management Team Approval Date:	0/0/00
Last Revision Date:	2/3/2020
Policy Update Responsibility:	Information Security Officer

Remote Worker Policy

Purpose

The purpose of the Network Center, Inc. Remote Worker Policy is to establish the requirements for the use of technology to access information and systems outside the Network Center, Inc. corporate or branch offices.

Audience

The Network Center, Inc. Remote Worker Policy applies to all Network Center, Inc. employees that have been designated as full-time remote employees or given permission by their supervisor to perform their normal work functions away from the office.

Policy

General

- Remote workers must be granted permission prior to working remote for extended periods
- All remote workers are required to review remote worker security training annually
- Remote workers must abide by existing polices and those described below

Connectivity

- Workers must limit the use of unsecured WIFI (public hotspots)
- All remote access must use encrypted methods to connect to corporate network or cloud infrastructure.
    - Site to Site VPN
    - Client VPN
- Any use of web-based technologies to access sensitive information are required to utilize encrypted protocols
    - (https)

- Local networks must be segmented from other non-work-related devices
    - When using a home network, utilize a separate VLAN segment work devices
    - If using a work provided firewall, only work-related devices are allowed to connect to and through it. All other devices must be located on a separate network.
- When using wireless from a home network, a minimum of WPA2 encryption must be used.

Local Device

- Devices must have antivirus/antimalware software installed and up to date
- Devices must have Automate deployed
- All media must be encrypted using current encryption standards
    - Laptops
    - Tablets
    - Mobile Devices
    - Removable Media.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 18
- NIST CSF: ID.GV, ID.RA, ID.RM, PR.IP

Waivers

Waivers from certain policy provisions may be sought following the Network Center, Inc. Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.