Remote Work Policy

PURPOSE

The purpose of this policy is to specify MCVO Remote Work Policy requirements as it pertains to remote worker options including alternative work locations and flexible work hours. This policy applies to any Company employee or contractor working at a location outside of offices owned or leased by Company whether planned or situational.

2. POLICY

2.1. Work Location

2.1.1. Each employee's approved primary remote work location is understood to be the home address on file with Human Resources. If the primary remote work location differs from the employee's home address on file, the employee must notify their manager for approval.

2.1.2. We understand that work may occur situationally outside of the primary virtual work location. It is incumbent upon the employee to ensure that alternate and situational work locations are suitable in assurance of compliance to Data Classification and Handling, Privacy, and Confidentiality policies and standards.

2.1.2.1. Locations generally open to the public such as coffee shops, restaurants, and airports are NOT suitable alternate work locations. There is a risk of distractions from background noise which can also impact web conferences. They're also unsafe for dealing with Confidential information as defined in Company's Data Classification and Handling Standard. Similarly, locations generally open to the public are not suitable for group gatherings to perform work in which sensitive information would be displayed on devices, would be distributed physically, or discussed verbally.

2.1.2.2. Remote work employees agree that they will conduct all business meetings at locations that ensure the confidentiality of company data as well as the confidentiality of clients, partners, and prospects.

2.1.2.3. Employees are expected to understand risks of insecure networks (rogue access points) and demonstrate heightened caution when connecting to public Wi-Fi access points.

2.1.3. Employees are required to have secure network connectivity at all work locations.

2.1.4. Company information must at all times be protected in a manner commensurate with its sensitivity and criticality and in compliance with applicable policies and procedures. Compliance requirements extend to both physical security and logical security. Remote work employees must take all necessary safeguards to ensure their alternate work site provides appropriate security and confidentiality of any and all data in accordance with the Business Ethics and Code of Conduct.

2.1.5. Company-provisioned devices, including but not limited to computing devices, phones, and cloud-services, must be used exclusively by the Remote work employees. Family members, friends, and others are not permitted to use Company devices. Remote work employees must never lend to others a handheld computer, credentials to Company systems or Company cloud-based services, or any other computer that stores information about Company business activities.

2.2. Device Security

2.2.1. Employees are to use approved Company-provided tools for purposes of productivity, debugging, and collaboration. The installation of software on Company-owned devices is prohibited without approval from Company's Technical Services team

2.2.2. Personal devices are prohibited from connecting to Company's corporate network. Personal devices may be used to access Virtual Desktop Infrastructure (VDI)

2.2.3. Personal devices are prohibited from downloading and/or locally storing Company or client information. It is understood by the employee that access to Company assets from personal devices will be limited and monitored to mitigate security risk.

2.2.4. All use of Company owned or managed assets, networks, cloud-based services, and data, is subject to productivity and/or security monitoring. There is no expectation of privacy while using Company owned or managed assets, networks, cloud-based services, and data. This includes anything you may access, view, create, store, transmit, or receive on or through such Company owned or managed assets, including any personal messages.

2.2.5. Any equipment provided by Company that is used to conduct Company business shall be kept in compliant work locations and may be used only by authorized employees.

2.2.6. Company is not responsible for support of non-Company owned or provided items or services

2.4. Business Continuity
2.4.1. Virtual workers must notify their manager, in a timely manner, of situations which impact their ability to complete their assigned duties including, but not limited to, Internet outages and power outages.
2.4.2. The virtual worker must identify alternate suitable work arrangements in the case of a localized Business Continuity situation that may affect the employee including, but not limited to, Internet outages and power outages.

3.Changes to Configurations and Software - On MCVO supplied computer hardware
3.1 Virtual workers must not change the operating system configuration or install new software. If such changes are required, they must be performed by Help Desk personnel with remote system maintenance software.
3.2 Changes to Hardware – Remote working computer equipment supplied by MCVO

must not be altered or added to in any way without prior knowledge and authorization from the Help Desk or the Management.

4. SCOPE
This policy applies to all MCVO employees, contractors and consultants who are considered to be working in a virtual or remote capacity as defined by virtual worker in this document.

5. RESPONSIBILITIES
All MCVO employees and affiliates are responsible for ensuring adherence to the requirements in this Policy when performing duties defined in the Scope above.

CONFIDENTIAL INFORMATION (Sensitive Information) – Any MCVO and MCVO Clients information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by MCVO from a Third-Party under a non-disclosure agreement.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of Employment or Contracts. MCVO reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

ACKNOWLEDGEMENT OF REMOTE WORK POLICY

I acknowledge that I have reviewed and understand the policy and guidelines within the document provided and discussed by the company during my orientation.
I understand it is my responsibility to comply with and implement all policy and procedures included in this document.

_____
Employee Printed Name and Signature

Date : _____