[Insert Logo]

Remote Work Policy

[ORGANIZATION\_NAME]

Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Policy Code: | 002 | Approved By: | {Insert} |
| Owner: | {Insert} | Effective Date: | {Insert} |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Created by | Description of change |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Purpose and Scope 4](#_Toc36546554)

[2. Introduction 4](#_Toc36546555)

[3. Roles and Responsibilities 4](#_Toc36546556)

[4. Authorization for Remote Work 5](#_Toc36546557)

[4.1 Remote Work Agreement 5](#_Toc36546558)

[4.2 Training 5](#_Toc36546559)

[5. Security for Remote Working Arrangements 5](#_Toc36546560)

[5.1 Use of Personally Owned Devices 6](#_Toc36546561)

[6. Management Considerations with Remote Work 7](#_Toc36546562)

[7. Policy Maintenance and Management 7](#_Toc36546563)

[8. References 7](#_Toc36546564)

[APPENDIX: REMOTE WORK AGREEMENT 8](#_Toc36546565)

[1. Purpose & Scope 8](#_Toc36546566)

[2. Who Must Comply with this Policy 8](#_Toc36546567)

[2.1 Existing Policies 8](#_Toc36546568)

[2.2 Security 9](#_Toc36546569)

[2.3 Scheduling 9](#_Toc36546570)

[2.4 Availability 10](#_Toc36546571)

[3. Statement of Acceptance 10](#_Toc36546572)

# Purpose and Scope

The purpose of this policy is to define [ORGANIZATION\_NAME]’s rules for remote working (i.e., when workforce members are engaged in the organization’s work while physically outside of the its office facilities). This topic may be referred to by a variety of terms, including telework, telecommuting, virtual work, or work from home.

This document applies to all [ORGANIZATION\_NAME] users.

# Introduction

Remote work may be offered by [ORGANIZATION\_NAME] for various reasons, such as to support life balance, allow flexibility, promote productivity, control facility space / costs, or help employees manage personal obligations. Remote work may also be required in some situations due to pandemic, natural disaster, or disruption at one of the organization’s facilities.

Remote work can create or exacerbate security risks to organizational assets and data. The safeguards defined in this policy are intended to protect the confidentiality, integrity, and availability of the organization’s information and information systems when work is conducted remotely.

# Roles and Responsibilities

|  |
| --- |
| Roles and Responsibilities |
| [Department Managers and Supervisors] | * Authorize specific roles or individuals to work remotely
* Provide those users the Remote Work User Agreement (see Appendix)
* Retain the signed agreement
* Establish regular communications with users working remotely to support a productive and healthy remote work arrangement
 |
| [Human Resources Manager] | * Include security requirements for remote work in regular security awareness training
* Work with department managers and supervisors to address any instances of non-compliance with the remote work agreement
 |
| [IT Director] | * Select and implement appropriate technical controls to address the risks of remote work
* Respond to user questions or needs regarding security while working remotely
* Ensure that disabling remote work mechanisms (i.e., VPN access, remote access to email) is included in standard off-boarding processes
 |

# Authorization for Remote Work

Only users who have been approved by their [Manager or Supervisor] may work remotely.

## Remote Work Agreement

All users authorized to work remotely are required to read and acknowledge [ORGANIZATION\_NAME]’s Remote Work User Agreement, which is included as an Appendix to this policy.

The agreement documents user requirements and responsibilities when working remotely, with the intent of addressing potential security risks to the organization’s information systems and assets.

## Training

Remote work security risks and requirements are included in the [ORGANIZATION\_NAME]’s regular security awareness training program. Users are encouraged to ask their supervisor or the IT department if they have any questions about remote work security or the controls in place to reduce risk.

# Security for Remote Working Arrangements

Remote work can introduce risk to the organization’s systems and data, especially in unprotected environments. This potential for risk requires the implementation of administrative and technical controls to manage those risks.

The [IT Director] is responsible for ensuring that appropriate technical safeguards are in place to address the risks of remote access.

Factors that should be considered when identifying risks and appropriate safeguards relating to remote working arrangements include:

* Communications security requirements, taking into account the need for remote access to the organization’s internal systems, the sensitivity of the information that will be accessed and passed over the communication link, and the sensitivity of the internal systems
* Physical security of sites where users will perform work remotely
* The threat of unauthorized access to information or resources by other persons at the remote location (e.g., family, roommates, friends)
* The use of personally owned devices, if the use of company-owned devices is not available to some or all users
* The use of personal email, if access to company email is not available remotely to some or all users
* The use of home networks and requirements or restrictions on the configuration of wireless and wired network services
* The use of cloud applications
* Issues relating to the organization’s software licensing agreements that may not permit such software to be used on workstations or other devices owned privately by users
* Malware protection and firewall requirements
* Procedures for backup and business continuity
* Audit and security monitoring (accountability)
* Revocation of authority and access rights, and the return of equipment when remote work or employment is discontinued
* Permitted and forbidden types of activities

[ORGANIZATION\_NAME] uses the following security controls to mitigate risks related to remote work:

* Virtual Private Network (VPN)
* Time-out of remote sessions and cloud applications
* Long, strong passwords
* Multifactor authentication
* Secure configuration of cloud applications
* Antivirus
* Encryption, at rest and in transit
* Secure methods for file-sharing
* Clear communication channels for security concerns or signs of suspicious activity to the IT team

## Use of Personally Owned Devices

The use of personally owned devices may be needed for remote work, especially when it is in response to an event such as pandemic or natural disaster. If personally owned devices will be used for remote work, [ORGANIZATION\_NAME] will implement a process to inform those users who are permitted to use such devices, along with rules and guidelines they must follow. In considering the use of personally owned devices for work purposes, [ORGANIZATION\_NAME] will consider appropriate security controls that should be in place as well as issue user guidance on secure remote work. Examples of security controls for personally owned devices include, but are not necessarily limited to the following:

* Full-disk encryption
* Long, strong passwords
* Current OS version and patching, with automatic updates enabled
* Anti-virus, with automatic updates enabled
* Physical security of devices
* Automatic screensaver / locking devices when unattended
* Requiring work-related files and applications to be closed if the device will be used by another person (i.e., family members)
* Restricting or prohibiting the storage of sensitive data on personal devices
* Mobile device management

# Management Considerations with Remote Work

Remote work arrangements require attention and communication to be productive and healthy for both the user and the organization. Managers and supervisors must establish consistent communications with users working remotely to help foster a positive remote work situation. Communication needs may include tasking, deliverables, status updates, scheduling, and more. Communication plans may include regular check-ins by phone, daily or weekly status emails, weekly progress reports, or a combination of strategies.

Managers should also take steps to maintain a sense of teamwork and collaboration. These steps may include regular team meetings, conducted remotely if needed, or requiring remote workers to call in to all regularly scheduled meetings. The use of chat applications, group conference calls, and video-conferencing can contribute to maintaining connections among teams and coworkers, and should be encouraged if they are authorized by the organization.

# Policy Maintenance and Management

The owner of this document must review and perform any necessary updates to this document at least annually, or may delegate tasks related to this policy as appropriate. Revisions must be communicated to relevant roles and users throughout the organization.

# References

**NIST Cybersecurity Framework References**

* ID.AM – Asset Management
* PR.AC – Identity Management and Access Control
* PR.AT – Awareness and Training
* PR.DS – Data Security
* PR.IP – Information Protection Processes and Procedures
* PR.PT – Protective Technology

**Policy References**

* Access and Authorization Policy
* Acceptable Use Policy
* Mobile Device Policy
* Information Classification, Handling, and Transfer Policy
* Asset Management

# APPENDIX: REMOTE WORK AGREEMENT

# Purpose & Scope

Remote work may be offered by [ORGANIZATION\_NAME] for various reasons, such as to support life balance, allow flexibility, promote productivity, control facility space / costs, or help employees manage personal obligations. Remote work may also be required in some situations due to pandemic, natural disaster, or disruption at one of the organization’s facilities.

Remote work can create or exacerbate security risks to organizational assets and data. This policy contains rules and guidelines intended to protect the confidentiality, integrity, and availability of the organization’s information and information systems when work is conducted remotely.

With the goal of making remote work a successful arrangement for both users and the organization, [ORGANIZATION\_NAME] has set the following requirements and expectations for remote work. This Remote Work Agreement must be reviewed and signed by all users who have been authorized by [ORGANIZATION\_NAME] for remote work.

# Who Must Comply with this Policy

All users are required to comply with this Policy. By signing and returning the Statement of Acceptance below, you acknowledge your understanding of, and willingness to comply with, all aspects of this policy.

##  Existing Policies

[ORGANIZATION\_NAME]’s existing policies continue to apply whether working in the office or remotely. This includes requirements documented in the Employee Handbook, Acceptable Use Policy, Data Classification Policy, and more.

Here is a summary of policies that users should keep in mind while working remotely.

* Do not attempt to bypass any security measures implemented by [ORGANIZATION\_NAME], (i.e., antivirus, password requirements, multifactor authentication, screensaver, restricted file access).
* Do not use organizational assets or network for prohibited activities, such as gambling, illegal activity, accessing adult content, operating your own business, or other activities generally considered inappropriate for work purposes.
* Use only approved methods for sending and receiving information.
* Only use approved software and applications, including cloud applications.
* Continue to pay attention to data classification, such as sensitive and confidential, and the associated requirements around handling, transmission, storage, sharing, and secure destruction.
* Do not use removable media unless you have been specifically authorized to do so. Never connect removable media if you do not know its source or owner.
* Remember that you do not have a right to privacy when using [COMPANY\_NAME]’s technology resources. Use may be monitored.

## Security

Primary considerations for users performing remote work include securing sensitive documents, physical protection of mobile devices, locking screens when unattended, preventing “shoulder surfing”, and taking care when conducting phone calls to ensure that company or client information is not overheard.

* Physical Security
	+ Physically safeguard all devices to prevent theft or damage. Do not leave devices unattended in vehicles, checked luggage, or publicly accessible areas.
	+ Prevent unauthorized viewing of your computer screen
	+ Lock computer screens when left unattended
	+ Secure documents when not in use
	+ Ensure work-related phone conversations and meetings cannot be overheard by others
	+ Establish a safe space dedicated to work free from potential hazards and conducive to a safe and healthy work environment
	+ Immediately report lost or stolen devices.
* IT Security
	+ Follow security requirements issued by the [IT Department or Security Officer], such as the use of VPN, long passwords, and multifactor authentication
	+ Do not connect directly to untrusted public networks, such as free wireless at coffee shops. Connect to a trusted network or VPN whenever possible.
	+ Watch for phishing emails, and be wary of phone calls asking you for information
	+ Keep passwords secure. Do not keep them on post-it notes or where others can access them. Never disclose passwords by email or phone
	+ Keep work and personal accounts separate, and do not reuse passwords between work and personal accounts
	+ Do not use applications or cloud services that have not been explicitly approved. If you have a specific work need (i.e., file sharing with clients), contact the [IT Team or Help Desk] for guidance
	+ Only use a personal device for work if you have been authorized to do so. If so, follow all security guidance from the [IT Director or your Manager], and be sure to close all work files and applications if the device will be used by someone else (i.e., family members). Periodically delete work files from the device when no longer needed.
	+ Immediately report anything suspicious to your [IT Team or Help Desk]

## Scheduling

If your remote work hours will vary from your usual office schedule, be sure to communicate your plan.

* Clearly communicate planned work hours and changes to plans to your supervisor and any coworkers who are likely to need to be in contact with you
* Work during the agreed upon work hours
* Notify your supervisor if your plans change due to illness, family needs, or any other circumstance that will require you to use time off rather than work as planned
* Accurately record work hours versus time off if your plans change
* Request remote work at least 24 hours in advance for planned occurrences, and as soon as possible for unplanned situations

## Availability

Take steps to be as available and responsive as you are in the office.

* Be available to your supervisor, coworkers, and clients during your planned work hours, by email, phone, text, and chat
* Notify your supervisor by email, chat, or text if you expect to be unavailable during the agreed upon work hours.
* Be proactive and go the extra mile to keep the lines of communication open with coworkers

# Statement of Acceptance

**By signing below, I acknowledge all of the following:**

1. I acknowledge that I have read and understand all sections of this Remote Work Agreement.
2. I understand that violation of this agreement may result in disciplinary action, up to and including termination of employment.
3. If I have any questions about these policies and procedures, I will ask my immediate supervisor or [ORGANIZATION\_NAME]’s [Help Desk or Security Officer].

Signature\*: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\* Note that remote work necessitated by a pandemic or facility/natural disaster may make a physical signature impractical. In such cases, an email acknowledgement may suffice. If needed, ask your supervisor or manager how to proceed.