Information Security
Working Remotely

|  |  |  |  |
| --- | --- | --- | --- |
| Policy ID |  | **Effective Date** |  |
| Version | 1.0 | **Contact** |  |
| Scope | Technology Services |  |  |

**Table of Contents**

1.0 Overview 1

2.0 Purpose 1

3.0 Scope 1

4.0 Definitions 2

5.0 Responsibilities 2

6.0 Assets 2

7.0 Connections 3

7.1 Virtual Desktop Infrastructure (VDI) – Primary Method 3

7.2 Virtual Private Network (VPN) – Limited Approval 3

8.0 Travel Considerations 3

9.0 Physical Security 3

10.0 Policy Maintenance 3

11.0 Related Policies 4

Revision History 4

# 1.0 Overview

Remote access to our Firm network is essential to maintain productivity, but many cases this remote access originates from networks with significantly lower security posture than the Firm’s network. While these remote networks are beyond the control of Firm Name, we must mitigate these external risks the best of our ability.

Information managed at Firm Name must at all times be protected in a manner appropriate with its sensitivity and criticality as defined in the *Information Classification Policy*. The precautions described in this policy apply regardless of the device used to connect, the location/network connection point, or the individuals who have access to the information. This means that workers must protect information in a similar manner no matter whether they are in a Firm Name office, a hotel room, or at a home office.

# 2.0 Purpose

The purpose of this policy is to define the rules and requirements for connecting to Firm Name’s network from any host. These rules and requirements are designed to minimize the potential exposure of the Firm and its client’s information.

# 3.0 Scope

This policy applies to all Employees, Non-Partner Attorneys, Partner Attorneys, and Third-Party Vendors.

# 4.0 Definitions

**Remote Access**: Accessing Firm Name systems from outside of the Firm’s premises with a firm-owned, personally owned, or publicly accessible computer, laptop, smartphone, or other device. The information accessed and processed continues to reside on the Firm’s systems.

**Mobile Device**: Any portable computing device (i.e., laptops, tablets, smartphones).

**Mobile Working**: Carrying out work as an employee of the Firm from outside of the Firm’s processes.

**Asset**: A device used to connect to the Firm network/systems.

# 5.0 Responsibilities

These guidelines aim to outline responsibility with regards to any remote access options provided by Firm Name, and when working with Firm Name information using mobile devices.

1. All approved/eligible users will be able to connect to the Firm Name environment remotely. This carries with it the responsibility to abide by the Information Security Policy, its principles, and any applicable supporting policies, procedures and guidance.
2. It is the responsibility of Firm Name employees, partners, contractors, and vendors with remote access privileges to the Firm’s network and information to ensure that their remote access connection is given the same consideration as any on-site connection to the Firm.

# 6.0 Assets

1. **Encryption** – Although primary storage and processing of information will be handled within a central virtual environment, it is understood that some situations will require temporary use of information on a firm laptop. All firm-issued laptops (i.e., assigned to a user), containing Confidential or Protected information must consistently employ both hard disk encryption and boot protection through a password. These two essential controls must be provided through software or hardware systems approved by the Security Team.
2. **Sharing Devices** – Two-form authentication fobs, laptops, mobile devices, fixed passwords, or any other access devices or parameters should not be shared with anyone without prior approval from the Security Team. This means that a remote computer used for Firm Name business must be used exclusively by the assigned user.
3. **Non-Firm Laptops/Desktops** – Storage and processing of any Firm Name information shall remain only within the virtual environment when using a non-Firm laptops or desktop.
4. **Changes to Hardware** – Laptops issued by Firm Name must not be altered or added to in any way without prior knowledge and authorization from Technology Services.
5. **Loaner Laptops** - A loaner laptop may be provided when available. Loaner computers may vary in performance and configuration. Loaners must be returned upon request and cleared of any locally saved information.
6. **Reporting Loss or Damage** – Any loss or damage to any laptop or other mobile device supplied by the Firm, or containing Firm information must promptly be reported to the Help Desk whom should report to the Security Team.

# 7.0 Connections

The guidelines below outline the Firm-approved processes for connecting to the Firm’s network remotely.

## 7.1 Virtual Desktop Infrastructure (VDI) – Primary Method

1. The Firm’s primary virtual desktop and connection to resources/systems is managed through virtual desktop infrastructure.
2. All authentications to VDI must utilize a username, fixed password, and the Firm’s in effect two-form authentication control.
3. Logins, PINs, and passwords should be protected at all time as stated in the Password Policy.

## 7.2 Virtual Private Network (VPN) – Limited Approval

1. VPN connections are only permitted on Firm-owned/managed devices unless otherwise approved by the Security Team.
2. All authentications to VPN must utilize a username, fixed password, and the Firm’s in effect two-form authentication control.
3. Logins, PINs, and passwords should be protected at all time as stated in the Password Policy.

# 8.0 Travel Considerations

1. Confidential or Protected information may not be removed from Firm Name premises unless the information’s Owner has approved in advance. This policy includes information stored on portable computer hard disks, CD-ROMs, and flash drive technologies.
2. Whenever Confidential or Protected information is carried into a foreign country, the information must be stored in some inaccessible form, such as an encrypted external storage media.
3. Firm Name and Client information must not be read, discussed, or otherwise exposed in restaurants, on airplanes, on trains, or in other public places where unauthorized people might discover it.

# 9.0 Physical Security

1. At alternative work sites, reasonable precautions must be taken to protect the Firm’s hardware, software, and information from theft, damage, and misuse.
2. Teleworkers shall use a shredder to appropriately dispose of printed versions of confidential or protected information.
3. The display screens for all systems used to handle Firm and client information must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means.
4. After completing a remote session, a log off and disconnect should be followed.

# 10.0 Policy Maintenance

The responsibility of ensuring this policy is kept current as needed for purposes of compliance with the Firm’s security requirements is assigned to the Security Team.

# 11.0 Related Policies

* Encryption Management
* Information Classification
* Password
* Vendor Management

# Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review Date | Reviewer/ApproverName |
| 1.0 | Initial Version |  |  |  |
|  |  |  |  |  |