

NOTE: This policy template is freely shared by SecurityStudio. Any/all modifications of this document are permitted; however, we request this template be shared freely with others in our attempt to help them with their information security challenges too. Everything we do at SecurityStudio is focused on our mission; *to fix the broken (information security) industry*.

**#MissionBeforeMoney**

INSTRUCTIONS: Modify all parts of this document to fit for your organization, including changing logos, format, and language. The most common mistake when using a template like this is to not reflect the culture of your organization. Replace all “(ORGANIZATION)” tags with your organization’s name.

This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](http://creativecommons.org/licenses/by-sa/4.0/).

Work from Home (“WFH”) Security Policy

To account for (ORGANIZATION) information security in the homes of our employees, contractors, and other 3rd-parties.

# Purpose

(ORGANIZATION) permits working from home for several reasons, chief among them being to protect the safety and well-being of personnel and as a convenience to personnel. Working from home presents unique information security challenges for (ORGANIZATION), and this policy communicates the minimum necessary precautions that must be taken to protect (ORGANIZATION) information.

# Audience

This policy applies to all employees, contractors, and 3rd-parties who provide services to (ORGANIZATION) while working from home.

# Definitions

The following definitions apply only to aid the understanding of the reader of this policy:

* **Employee** – defined as a person who is a part-time or full-time hourly or salaried employee who is performing work for (ORGANIZATION) as an employee, and not an independent contractor. Sometimes referred to as a “W2 employee”.
* **Contractor** – defined as a person or organization who is performing work for (ORGANIZATION) as an independent contractor or organization. Sometimes referred to as a “1099 worker”.
* **3rd-party** – any other person or organization who provides a service or product to (ORGANIZATION) and does not necessarily fit the definition of “contractor” or “employee”.
* **Home** – the location where a person resides or lives, not owned or wholly-managed by (ORGANIZATION).

Collectively, “employee”, “contractor”, and “3rd-party” will be referred to as “personnel” throughout the remainder of this document.

# Policy

The policy is organized into three sections; general, physical, and technical according to the precaution or requirement specified.

## General

* Personnel understand that working from home is a privilege granted by (ORGANIZATION) that may be revoked at any time.
* All personnel working from home on behalf of (ORGANIZATION) must be explicitly authorized by (ORGANIZATION).
* Information belonging to (ORGANIZATION) must be protected according to all other information security policies.
* Personnel are responsible for understanding which information assets (computers, mobile devices, accounts, data, etc.) belong to (ORGANIZATION) and which do not.
* Personnel will maintain separation of (ORGANIZATION) information assets and personally owned information assets at the direction of (ORGANIZATION), where feasible.
* Personnel will actively participate in all training and awareness exercises provided by (ORGANIZATION) related to work from home information security.
* (ORGANIZATION) will provide a personal information security assessment tool for all personnel to foster better personal and family protection.
* Personnel will complete a proper evaluation of their personal information security habits and abilities, providing anonymous results to (ORGANIZATION) for continued improvement.

## Physical

* Physical safety of personnel and/or personnel family members is of utmost importance to (ORGANIZATION); data protection is always secondary to safety.
* The physical location where (ORGANIZATION) work is performed must be equipped with adequate fire monitoring and/or suppression, in accordance with local fire codes.
* (ORGANIZATION) information assets must be maintained in a locked building, room, and/or cabinet when personnel are not in close physical proximity.
* (ORGANIZATION) information assets must not be left unattended in a vehicle within plain sight of passersby.
* The loss or theft of any (ORGANIZATION) information asset must be reported to (ORGANIZATION) immediately, but only after physical safety of personnel and family members is assured.
* Work done on behalf of (ORGANIZATION) must be performed in a dedicated location within the home; a dedicated office or workspace separate from other activities occurring in the home.

## Technical

* (ORGANIZATION) information assets are not to be used for personal business or entertainment.
* Computers and/or mobile devices that are not owned and/or adequately controlled by (ORGANIZATION) are not permitted for use with (ORGANIZATION) information assets.
* Use of (ORGANIZATION) information assets is restricted to authorized personnel only.
* Personnel must report information security related incidents to (ORGANIZATION) regardless of its direct effect on (ORGANIZATION) information assets.
* Default passwords and/or authentication on all network devices used in conjunction with (ORGANIZATION) information resources have been changed in accordance with the (ORGANIZATION) Password Policy.
* All network traffic for remote access to all (ORGANIZATION) information assets must be encrypted.
* Remote access to all (ORGANIZATION) information assets is permitted only through methods that are explicitly authorized by (ORGANIZATION).
* (ORGANIZATION) information assets must be encrypted to protect all data at rest.
* Personnel agree to comply with any/all additional information security related requirements given by (ORGANIZATION) to protect (ORGANIZATION) information assets.

# Waivers

Waivers from certain and specific policy provisions may be sought following the (ORGANIZATION) Waiver Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted.

# Enforcement

This Work from Home (“WFH”) Security Policy supplements and compliments all other work from home and information security related policies, it does not supersede any such related policy or vice versa. Where there are any perceived or unintended conflicts between (ORGANIZATION) policies, they must be brought to the attention of (ORGANIZATION) for immediate reconciliation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

# Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Modified Date** | **Approved Date** | **Approved By** | **Reason/Comments** |
| 1.0.0 | September, 2020 | September, 2020 | John Doe | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |