azcomp TECHNOLOGIES

(replace with your own logo or letterhead)

Work from Home Policy Template

Objective of Working from Home:

[Use this section to define your objectives for allowing the employee to work from home]

Example:

Telecommuting allows employees to work remotely at home during the COVID-19 pandemic. It is not an entitlement, it is not a company-wide adjustment and may be reversed after the pandemic subsides, it in no way changes the terms and conditions of employment with [company]. Those who work from home have an increased responsibility to show integrity while in the privacy of their home. Their job duties and functions are unchanged and should be carried out in a manner that is equivalent to when the employee was in the office.

Consistent with the organization's expectations of information security for employees working at the office, telecommuting employees will be expected to ensure the protection of proprietary company and customer information accessible from their home office. Steps include use of locked file cabinets and desks, regular password maintenance, shredder, and any other steps appropriate for the job and the environment. Do not save company passwords on your computer or in web browsers.

The employee will establish an appropriate work environment within his or her home for work purposes. The organization will not be responsible for costs associated with initial setup of the employee's home office such as remodeling, furniture or lighting, nor for repairs or modifications to the home office space. Employees will be offered appropriate assistance in setting up a workstation designed for safe, comfortable work.

The organization will determine, with information supplied by the employee and the supervisor, the appropriate equipment needs (including hardware, software, modems, phone and data lines, facsimile equipment or software, and photocopiers) for each telecommuting arrangement on a case-by-case basis. The organization accepts no responsibility for damage or repairs to employee-owned equipment. The organization reserves the right to make determinations as to appropriate equipment, subject to change at any time. Equipment supplied by the organization is to be used for business purposes only. The telecommuter should sign an inventory of all office property and agrees to take appropriate action to protect the items from damage or theft. Upon termination of employment all company property will be returned to the company, unless other arrangements have been made. Once all needs are understood, the organization will work with the employee under one of the following scenarios:

1. Equipment will be supplied by the employee, if deemed appropriate by the organization, and will be maintained by the employee
2. Equipment will be supplied by the organization and will be maintained by the organization
3. Equipment will be purchased by the employee at their own expense from the organization (at cost) and will be maintained by the organization

(replace with your own logo or letterhead)

Employee Owned Computer Security Requirements:

1. The employee must have a device that the employee will dedicate for business purposes only
2. The employee must ensure the device drives are encrypted – this can be accomplished by using either Microsoft BitLocker (requires Windows 8, 8.1, or 10 Pro) or Apple FileVault on macOS
3. The employee must install [insert preferred antivirus program here] to protect the device – you can download it here: https://home.sophos.com/en-us.aspx.
4. The employee must turn on Automatic Updates
5. The employee must have a password protected account on the computer
6. The employee must use a strong password that is at least 12 characters or more with an uppercase letter, a lowercase letter, a number and a symbol – this password does not need to be changed unless there is suspicion that the password has been compromised
7. The employee must have a password protected screen lock timeout set to a maximum of 15 minutes
8. The employee must make sure wireless router traffic is encrypted using (at a minimum) WPA2-AES encryption
9. The employee must make sure that the password to the wireless network is a strong password that is at least 12 characters or more with an uppercase letter, a lowercase letter, a number and a symbol
10. The employee must **never** download or print PHI – no footprint (evidence of PHI) will be allowed at Home Offices
11. The employee must conduct the physical site audit (end of this document) and provide the details of the audit to the current Security Officer every 12 months
12. If the above are not followed, the employee must defend their decisions to the Department of Health and Human Services (HHS) should a breach occur, and it be revealed that these protocols were not followed
13. The employee must allow a member of the organization's IT department confirm all requirements are in place before access to company resources are granted

azcomp TECHNOLOGIES

(replace with your own logo or letterhead)

Home Office Site Audit

Questions completed by Employee:	Yes	No	N/A	Notes
Do you store paper documents that contain Protected Health Information in your home office?	○	○	○	
Do you print paper documents that contain Protected Health Information at your home office?	○	○	○	
Do you receive paper faxes at a physical fax machine in your home office?	○	○	○	
Do you take paper or electronic files containing Protected Health Information to your home office?	○	○	○	
Do you lock the door to your home?	○	○	○	
Do you lock the door to your home office?	○	○	○	
Do you have an alarm on your home / home office?	○	○	○	
Questions completed by the IT Department:	**Yes**	**No**	**N/A**	**Notes**
Is the computer centrally managed by AZCOMP?	○	○	○	
Is the drive on the computer encrypted using either Apple FileVault or Microsoft BitLocker encryption?	○	○	○	
Is Sophos Home Premium or Sophos Intercept X Advanced installed?	○	○	○	
Are automatic updates turned on?	○	○	○	
Is the computer password protected with at least a 12-character complex password?	○	○	○	
Is the computer set to lock after a maximum of 15 minutes of inactivity on the computer?	○	○	○	
Does the employee have a Wireless Router?	○	○	○	
If they have a Wireless Router is it protected using WPA2-AES and a strong password?	○	○	○	

Signed and Agreed to by:

Employee Signature: _____ Date: _____

Print Name: _____ Title: _____

Supervisor Signature: _____ Date: _____

Print Name: _____ Title: _____