This is a sample BYOD policy with language incorporating the considerations discussed. It is provided only as an exemplar and is not intended to be used without modification to fit your particular operational situation. Also, the sample policy should be modified to conform with any relevant law particular to your state or local jurisdiction. For a copy of the policy, contact Nicole Upano at nupano@naahq.org.

Bring Your Own Device (BYOD) Policy

The Company has adopted this Bring Your Own Device (BYOD) Policy to meet the needs of our employees. Using your own device for work purposes is not a right, and must be authorized by the Company. In addition, you must read, sign and follow this policy at all times in order to use and continue to use your personal device for work purposes.

Network and Information Security

- Access sensitive business data through Company e-mail and approved applications only. These access points are protected through the security controls discussed below. In all other respects, keep sensitive business data off of your personal device. Sensitive business data includes all documents or data whose loss, misuse, or unauthorized access could adversely affect the privacy or welfare of an individual or Company operations. Delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments. Company IT will provide instructions for identifying and removing these unintended file downloads. When in doubt, delete it off of your device;
- Maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer and requested by IT. No "Jail Breaking" the device (installing software that allows the user to bypass standard built-in security features and controls);
- Do not share the device with other individuals or family members. This is strictly prohibited due to the business use of the device (potential access to Company e-mail, etc.). If you are in a situation where you need to share your device with another person, please let the Company know and Company IT will evaluate whether to provide you a Company-issued device;
- Agree to allow the installation of mobile device management software by Company IT. This software allows the Company to remotely locate and wipe the device if it is lost or stolen.
- Report lost or stolen devices to Company within 4 hours or as soon as practical after the device is noticed missing. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- Report any suspected unauthorized access of the device or data breach immediately.
- Your device may be remotely wiped if:
  - It is lost or stolen
  - You separate from your employment without first permitting IT to inspect your device
  - IT detects a data or policy breach, a virus or similar threat to the security of the Company's data and technology infrastructure, as determined by Company in its discretion.
- Smartphones and tablets that are not on our list of supported devices are not allowed to connect to the network. Current devices approved for use:
  - Android Smartphones & Tablets, OS version 7.0 or higher
  - iOS iPhones & iPads, iOS version 10 or higher
  - BlackBerry Smartphones & Playbook, BlackBerry 10 OS or higher
- All devices must be password protected and must lock themselves if idle for more than 2 minutes. You must comply with all Company password policies, including the use of strong passwords, password expiration and password history.

Wage and Hour Compliance

- **Overtime.** Consistent with Company Policy, all overtime work must be approved in advance by a supervisor. Non-exempt employees are paid for all hours worked in accordance with applicable law. Non-exempt employees are responsible for accurately recording their time and are prohibited from working off the clock. Non-exempt employees must have a legitimate business reason for accessing Company network, including Company e-mail, after working time and must receive advance authorization to do so, except in the event of an emergency. Working off the clock, in any form, is strictly prohibited. Any non-exempt employee who works after hours without advance authorization will be paid for such work, but is subject to discipline.
- **Meal Periods and Rest Breaks:** All rest breaks and meal periods are "off-duty." You will be relieved from all work-related duties and free from any Company control during your rest breaks and meal periods. Employees should not conduct any work-related activities during their rest breaks or meal periods, including sending or responding to work-related emails or texts. You are not required to remain "on-call" during your rest breaks or meal periods, unless you are specifically designed as on-call by your supervisor.
- **Dollar Amount of Reimbursement:** Authorized users of personal devices will receive a reimbursement as follows:
  - Voice only - $[XX] per month
  - Data only - $[XX] per month
  - Voice/Data - $[XX] per month
- **Process for Reimbursement:** Complete the Mobile Device Reimbursement Request Form and submit it to your supervisor for approval. Your supervisor will determine if the request meets the criteria and intent of the policy.
- **Reimbursement:** Payment will be made upon presentation of a completed Personal Reimbursement Form along with a copy of the monthly device bill.
- **Use of Device:** You must retain an active device as long as you are receiving device reimbursement. The device may be used for both business and personal purposes, consistent with this policy. Extra services or equipment may be added at your expense. You will not be eligible for device reimbursement during a leave of absence.

Policy and Procedure Compliance

- **Compliance with Company Policies.** You are expected to use your device in an ethical manner at all times and adhere to the Email and Internet Use and other applicable policies as outlined in the Company handbook. This also includes Company policies related to mobile device use while driving and other Company IT policies outlined in the Company handbook.
- **Policy against Harassment:** Displaying sexually explicit images unrelated to work related projects on Company property is a violation of the Company's policy on sexual harassment. You are not allowed to download, archive, edit, or manipulate sexually explicit material while using Company resources, including Company wireless networks, unless relevant to a work related project with approval from your immediate supervisor. If you receive material from outside sources that are sexually explicit and not relevant to work related projects, it is wise to delete or destroy it. If the originator of this material is an employee, you should notify the employee's supervisor or Human Resources. If you believe you have been harassed or if the employee persists in sending the material, you should report the incident immediately in accordance with the Company's Discrimination, Harassment, and Retaliation Prevention Policy.

Employee Privacy

- Company will respect the privacy of your personal device to the extent it is not used for work purposes, and will request access to the device for business purposes only, such as access by technicians to implement security controls, to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads Company email/attachments/documents to their personal device), to protect company intellectual property, or for other business purposes. If you have concerns related to compliance with our security requirements, you may opt to drop out of the BYOD program.
- We will take reasonable precautions to prevent your personal data from being lost in the event we must remote wipe a device. However, we cannot guarantee that such data will be saved, and are not responsible for any expenses or damages that result from the loss of personal data. It is your responsibility to take additional precautions, such as backing up contacts, pictures, messages, etc.

Miscellaneous

- The Company is not responsible maintaining or repairing your mobile device
- The Company is not responsible maintaining, repairing, or reinstalling, any personal software or personal apps on your device

USER ACKNOWLEDGMENT AND AGREEMENT

I acknowledge, understand and will comply with the BYOD Policy. I understand that addition of Company-provided third party software may decrease the available memory or storage on my personal device and that Company is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device in this program. I understand that contacting vendors for trouble-shooting and support of third-party software is my responsibility, with limited configuration support and advice provided by Company IT.

Upon the termination of employment, at any other time that the Company requests, or if I elect to discontinue my participation in the BYOD program, I will: (1) immediately refrain from accessing any Confidential Information stored on my device; (2) allow the Company access to retrieve any Company information or documents stored on my device; and (3) if and when so directed by the Company, permanently delete and erase any Company documents or information stored on my device or provide access to allow the Company to do so; and (4) allow the Company access to the device to remove and disable any Company provided third-party software and services from it.

Employee Name: _____

Employee Signature: _____ Date: _____