[ORG] Policy and Employee Agreement on
Bring Your Own Device ('BYOD')

The policy below is in place to help protect the security and integrity of [ORG]'s client's data and information.

The employee (you) MUST agree to the terms and conditions below in order to use your mobile device, laptop and/or home computer, and/or tablet (personal device(s)) for the purposes of business activities.

This policy applies to work performed on a personal device(s) for [ORG] during working and nonworking hours.

Acceptable Use

- Business use during work hours includes emailing, calling, and other activities that support the activities of [ORG] and its clients.
- Personal use during work hours includes family and emergency phone calls and limited recreation during breaks.
- You may access email, documents, calendar, and other work product, information, and data controlled by [ORG] and such information owned by [ORG]'s clients from your personal device(s).

Non-acceptable uses during work hours include:

- Engaging in outside business activities
- Social or recreational activities outside of breaks
- Anything else that would violate the employee agreement
- OPTIONAL: Political actives as restricted by LSC grant rules

Conduct Not Prohibited by This Policy

This policy is not intended to restrict communications or actions protected or required by state or federal law.

Device and Support

- IT will provide [no/limited/full] device support for your personal device(s).

Security

Devices must:

- Maintain antivirus software
- Enable remote wiping on your personal device(s) by [yourself/IT] if your device becomes missing or is stolen.
- Feature a locking mechanism;
    - Acceptable locking mechanisms include PIN, password, or biometrics (fingerprint or facial recognition). We (strongly encourage/ require) PIN or Password.
    - Device must be set to automatically lock if idle for a period of [X] minutes, and device use must be suspended after [X] failed login attempts.
- You must use a password manager, we recommend LastPass which has a free version.
- OPTIONAL [ORG] will reimburse or pay for Password Manager [X]

· You must:

- Remove all client information and other information and data related to [ORG] from your personal device(s) when such work is complete and on termination of your employment with [ORG].
- Inform [ORG] if your personal device(s) becomes missing or is stolen within 24 hours.
- Protect all client information on your personal device(s).

Employee's Responsibilities

- You assume full responsibility for ensuring the protection of client information and data your personal device(s).
- You assume full responsibility for all risks of using your personal device(s) for business purposes, including but not limited to loss of client, company, and personal data or programming errors that render the device unusable.

Reimbursement [IF APPLICABLE]

- *Option 1* – [ORG] will not reimburse you for any device-related expenses.
- *Option 2* – [ORG] will provide you a monthly stipend of $[X] for a data plan on your personal device.

Disclaimer

- [ORG] is not responsible for your personal device(s).
- [ORG] reserves the right to change this policy and will inform you of any changes to this policy through e-mail and updates to the employee handbook.
- Under state and federal laws, [ORG] is required to disclose any breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. [See applicable local, state and federal rules for your ORG - refer to RCW 19.255 for Washington state]
- [ORG] reserves the right to take disciplinary action for noncompliance with this policy.

[ORG] is not responsible for the loss of personal data and information.

By signing below, _____, employee of [ORG], understands and agrees to the policies and procedures outlined above.

_____ Date _____

Employee

_____ Date _____

Employer