[redacted]

Last revised by LP Sept 2020

1. All computers and information technology (IT) systems owned by [redacted] belong to [redacted] and are for business use. They may be assigned to specific staff, but may be used by staff only as authorized by [redacted]. [redacted] reserves the right to access and control all devices, software and data.

2. Purchasing of [redacted] computers and IT systems: purchases of all IT equipment must be approved by the IT Specialist. This includes computers and laptops. This does not include printers and printer toners.

3. Assigned workstations in the office: every staff should have a working computer. If your computer is not working properly, contact the IT Specialist right away. Save your work and turn your workstation off at the end of each day, unless there is some reason to leave it on.

4. Server: each office has a server. The directing attorney of each office should instruct staff to leave the server on at all times, unless otherwise instructed by the IT Specialist. The directing attorney should make sure the server has a good battery backup in case of power failure, so the battery can supply enough power for the server to shut down normally. (If the server shuts down suddenly, it can damage the server.)

5. Laptops: each office has a number of laptops. Laptops in each office are assigned to the office directing attorney. The director may re-assign a laptop for use by a particular staff, or may allow the laptop to be used by multiple people.

6. Cell phones:

    a. each office has a number of cell phones. Cell phones in each office are assigned to the office directing attorney. The directing attorney may re-assign a cell phone for use by a particular staff, or may allow the cell phone to be used by multiple staff.

    b. All [redacted] cell phones must be set to enable geolocation, so a supervisor can monitor the geographic location of each cell phone.

c. Use of Whatsapp on [redacted] cell phones: Please set up and use the WhatsApp Business app for use on [redacted] cell phones

7. Care of cell phones and laptops: Staff who use [redacted] cell phones and laptops are responsible for their proper care. This includes:

   a. Transporting them safely, with proper cases.

   b. Maintaining physical security to prevent theft and unauthorized use. Do not leave in a car. Do not leave unattended.

   c. Maintaining password security—phones and laptops when not in use should have the screen locked so that they cannot be used without a password. Do not provide your password to anyone except as authorized by your supervisor.

8. Driving with an [redacted] cell phone: all staff are strictly prohibited from using [redacted] cell phones when they are driving.

9. Personal use of [redacted] computers: All computer and technology equipment, systems, and data are provided for business use. Subject to their supervisor, and as limited below, staff may use [redacted] computers for limited personal use on their own time, so long as that use is consistent with all provisions of this policy, and does not interfere with business use. Permitted occasional personal use is subject to viewing, monitoring, or recording by [redacted]. [redacted] may further limit personal use of its computers by employees from time to time as it sees fit by notice given to its employees.

10. Security of [redacted]'s IT: every employee is responsible for ensuring the security of [redacted]'s IT, which includes client confidential information. Security measures to be followed by all staff, include:

    a. Physical security: keep [redacted] equipment secure so that unauthorized users do not have access to the server, workstation, laptop, cell phone, or other device.
    b. Password security:
        i. All devices—computers, phones, laptops—must be password protected to prevent unauthorized access.
        ii. Log out or shut off your device when leaving your device unattended.
        iii. Use different passwords on different systems. For example, a Windows account password should not be the same as an Email password.

iv. Passwords used on company systems should never correspond with employee personal account passwords
v. Do not write passwords down. Use your [redacted] Google account to save your passwords for work. See, https://support.google.com/accounts/answer/6208650?hl=en
vi. Keep your personal and [redacted] passwords separate. Do not save your personal passwords on your [redacted] google account. If you have a personal google account, do not save [redacted] passwords on your personal google account.
vii. Do not use easy to guess passwords. Use the passwords suggested by Google, or other strong passwords.

11. Lost or stolen device: If any device is lost or stolen, report this to IT immediately. The device will be remotely removed from the web server's device list so that any access to e-mail will be prevented. Staff will also be asked to change their e-mail password.

12. How to access [redacted] data from outside the office:

    a. [redacted] cell phones and laptops can be used to access [redacted] data. There are 3 ways to do this:
        i. Google Drive: logging into your [redacted] Google account will give you access to Google Drive. This includes your [redacted] Drive folders, and the [redacted] Shared Drive folders. When properly set up, this should provide access to all your [redacted] data, including email, except for Prime.
        ii. Remote access to your desktop computer. You can ask IT for this. This will allow another computer (laptop, cell phone) to see and operate your desktop. You will have access to everything on your workstation in the office. Your workstation must be on for this to work. There is no way to turn on your workstation remotely.
        iii. VPN: if the above two methods are not available to get you what you need, IT can set up a VPN connection to the server in your office. Because of security risks of connecting a device that is outside the office to the office server, only devices which are used exclusively for [redacted] business may be used for this purpose. Any [redacted] device which has been used for any personal use, including personal email, any non-[redacted] downloads of any kind, including files such as MP3, videos, documents, and photos, are not to be used for VPN connections.

13. Keep work and personal identities separate. We are the same person at work and when we are off work, but it is important to recognize the difference between when we are communicating on behalf of the [redacted], and when we are speaking on our own and not connected with [redacted]. To that end:
    a. Do not send personal e-mails from your [redacted] email account.
    b. Do not send [redacted] e-mails from your personal email accounts.
    c. Facebook: Avoid using your personal Facebook account for [redacted] business. [redacted] has an [redacted] Facebook page, and any staff who desire to message with clients or others regarding [redacted] business can do so if they are designated as a "moderator" of the [redacted] Facebook page. Ask the Executive Director if you want to be a moderator. Each office should have at least one person designated as a moderator for this purpose. The [redacted] Facebook page is administered by the Executive Director and their designee, if any.
    d. Whatsapp: use the WhatsApp Business app on [redacted] cell phones to communicate regarding [redacted] business.

14. Use of personal devices for [redacted] business: personal cell phones, tablets, laptops, computers—all devices—may be used to:
    a. Access your [redacted] Google Drive account;
    b. With approval and assistance from IT, connect remotely to your workstation at the office;
    c. Receive and send [redacted] e-mail on [redacted] e-mail account.

    If you use your personal device for [redacted] business, you must ensure [redacted] data is protected using physical and password security protocols described above.

    Using your personal device for [redacted] business increases the risk that [redacted] data will be compromised. For example, an [redacted] filed can become infected by a virus that is on your personal device, and that file can infect other [redacted] files.

    DO NOT USE YOUR PERSONAL DEVICES FOR [redacted] BUSINESS IF YOU ARE NOT CONFIDENT THAT YOU CAN PROTECT [redacted] DATA.

15. Use of [redacted] Google Drive: [redacted] uses Google Drive for storing, sharing, and backing up data. Each staff person has an [redacted] Google account, which should be used as follows:
    a. Personal data, not connected to [redacted]: do not use [redacted] Google account for any personal data.
    b. [redacted] data that you don't want or need to share with anyone else at [redacted]: save all this data on your [redacted] Google Drive account. Note: [redacted] will still have access to this data, so don't use this for any personal data.

c. [redacted] data that should be shared within your office, including work on cases: save this data to the [redacted] Shared Drive for your office, using the following folders:
    i. Cases
        1. [subfolder] Open
        2. [subfolder] Closed
    ii. Community education, outreach, collaboration
    iii. Admin/management
    iv. Staff training
    v. Projects
    vi. Forms and templates
    vii. Shared with central office

    In Central office, Shared Drive uses the following folders for sharing documents within central office staff:
        i. Accounting
        ii. Development
        iii. IT
        iv. Management
        v. Human Resources

d. Document naming convention: all documents should be saved using the following protocol:
    i. Client documents: Client names; description of document. For example: William Pitmag affidavit re employment
    ii. Other docs: year of document; description. For example: 2020 letter to attorney general re human trafficking task force
    iii. When naming documents, please think about how you or someone else might search for these documents later, using words in the title of the document.

16. Added limitations on personal use: In addition to the above limitations, staff may not use [redacted] computers or other technology for any illegal purpose; for gambling; for anything pornographic.

17. All [redacted] employees shall take all reasonable precautions to preserve and protect [redacted] technology and computer equipment, systems, and data. This includes ensuring the physical safety of equipment and the privacy of passwords.

18. All [redacted] employees shall avoid computer scams that might compromise our equipment, systems, and data. Our primary defense against viruses, hacking attempts,

etc is our staff being wary and savvy. If in doubt about a website or e-mail, please check with our IT Specialist before clicking on suspect links or opening suspect attachments.

19. Use of thumbdrives/flash drives: do not use without the express permission from our IT Specialist. Do not use these to backup data. Do not use these to transfer data. There are too many security risks involved with the use of thumbdrives.

20. No [redacted] provided software may be deleted from and no non-[redacted]-provided software may be installed on any electronic property described in this policy without the express consent of the Directing Attorney of the [redacted] office involved. The Directing Attorney will give his or her consent only after consultation with the [redacted] Information Technology Specialist. Any decision by a Directing Attorney in this regard is subject to the review and final decision of the Executive Director.

21. [redacted] website: [redacted] maintains a website. All content on the [redacted] website must be approved by the Executive Director.

22. Any disregard or violation of [redacted]'s Computer Use Policy as set out in this policy may be subject to the warning, suspension, and termination procedures set forth in the Personnel Manual.

23. All [redacted] employees, board members, interns, and volunteers shall agree to abide by the terms of this Computer Use Policy by signing and dating a copy as indicated directly below. The executed copy of the agreement will then be placed in the employee's personnel file. [redacted] may make minor changes to and issue implementation procedures for this policy with written notice to those to whom the measures apply but without re-execution of this document.

24. I acknowledge that [redacted] has provided me the following [redacted] devices. I agree to care and use them in accordance with this policy.

Computers: Brand: _____

Model:_____

Serial Number:_____

Laptops: Brand: _____

Model:_____

Serial Number:_____

Phones: Brand: _____

Model:_____

Serial Number:_____

Tablets: Brand: _____

Model:_____

Serial Number:_____

Other: Brand: _____

Model:_____

Serial Number:_____

READ AND AGREED TO BY: _____ _____

Print name Signature

DATE: _____