[redacted] Technology Policy

The [redacted] is a large legal aid program with numerous technology solutions in place to meet the varied needs of our staff and clients. It is imperative that all employees be familiar with our Technology Policies and abide by them. Managers, please ensure that you go over these with new staff and students at onboarding. If anyone has questions, please contact [redacted]. Thank you for doing your part to ensure that our equipment is taken care of and our policies are followed - it will significantly increase the security of our systems and sensitive client data, reduce the amount of technology problems people encounter, and keep our services operational.

I. OWNERSHIP OF PROGRAM EQUIPMENT AND TECHNOLOGY

A. **Ownership.** All [redacted] equipment and technology is owned by [redacted] and subject to monitoring by IT staff and management. All technology systems, including computers, computer software, telephone systems, fax machines, copier machines, voicemail systems, email systems, and Internet access systems within the [redacted] offices are the sole property of [redacted] No individual staff member has any proprietary or confidential interest in any materials stored or copied in any office files or systems, including voicemail and email. Any material in any [redacted] system may be monitored, copied, or purged by the program management at any time. Additionally, staff should not store non-work-related files on their computer hard drives or on a [redacted] network.

B. [redacted] **Access to** [redacted] **Devices.** In order to assure that the primary use of these systems is the provision of legal services to the poor in compliance with program policies, program priorities, and program grant requirements, [redacted] has the right to monitor and control the use of all its property, equipment, and systems. [redacted] may access all aspects of all systems, without the consent of the user, at any time. The specific circumstances when [redacted] may access equipment include but are not limited to:

1. When necessary to identify or diagnose system or security vulnerabilities and problems or otherwise preserve the integrity of any system; or
2. When such access to systems is required to carry out essential business functions of [redacted]; or
3. When there are reasonable grounds to believe that a violation of law or a significant breach of [redacted] policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or
4. When the user's employment at [redacted] has ended and there is a business reason to access the system.

C. **Installing Software on** [redacted] **Devices**. [redacted] staff may install any applications or software on their assigned device which is available on the Company Portal. Before installing any other applications or software (not available on the company portal) on their assigned device, staff must request permission from both their managing attorney and [redacted]-IT. Any new applications or software must be installed by [redacted]-IT unless they have specifically designated this task to an office Computer Responsible Person (CRP). Adding an application or software to a shared device can only be done by [redacted]-IT after being requested by a Managing Attorney.

D. **Care of Program Equipment**. Staff are expected to exercise great care for [redacted] equipment. This includes: not eating or drinking near your keyboard or laptop; carrying laptops in protective cases; keeping laptops secure at all times and storing at proper temperatures; all cords should be used and stored so they won't be damaged or create trip hazards; etc. When [redacted] loans equipment to an employee (i.e., projectors or office laptops), the equipment is to be returned in its original condition.

This includes all peripherals and accessories (mice, cables, remotes, etc). The program may charge staff the cost of repair for the loss of or damage to program property if the damage is caused by actions of staff that are intentional, negligent, or in violation of this policy. In the event [redacted] equipment should be stolen, misplaced, or compromised in any way, employees are required to contact [redacted] and [redacted] IMMEDIATELY at [redacted]

E. **USB Keys**. Some employees and students are given a USB security key to enable access to shared laptop or desktop computers. Replacement of a lost security key will result in a $20 fee to the employee to cover the cost of a new key. Local Managing Attorneys (who may delegate this task to the CRP) will assign USB security keys to students and track the return of them at the end of the term. Any employee or student who loses their security key or does not return it is responsible for the $20 fee.

F. **Personal Use of [redacted] Equipment and Technology**. Employees are permitted reasonable personal use of program equipment provided that:

- this use occurs on the employee's personal time;
- the employee reimburses the program for any direct costs associated with the use;
- this use doesn't interfere or conflict with any other provision of this policy or with [redacted]'s programmatic use of the property, equipment, or systems.

Excessive use of technology resources for non-work-related purposes, such as game playing or downloading media files is prohibited. [redacted] email accounts are to be used for [redacted] program purposes only; staff are expected to have a non-work email account for their personal email correspondence.

G. **Prohibited uses of [redacted] Equipment and Technology**. For profit use of [redacted] equipment and technology is strictly prohibited. [redacted] employees are not permitted to use [redacted] equipment for for-profit purposes at any time. [redacted] employees are not permitted to use [redacted] equipment for LSC-prohibited purposes at any time. [redacted] employees are not permitted to let anyone who is not a [redacted] employee use [redacted] equipment.

H. **Assignment and Use of Shared Laptops**. All offices have one or more office laptops intended to be shared by staff ("shared devices"). The laptops can be checked out by any employee needing a laptop for a specific event or while their primary device is out of service. Shared laptops are not to be used for general daily use, or taken home (except between days of continuous use) - they must be available for general office use. Each office manager (who may delegate the task to the CRP) must track the location and working order of shared laptops at all times.

II. INTERNET USE

A. [redacted] **Internet - Work Related Use Only**. The program's connection to the Internet exists to assist us in our legal work, such as contacts with funders, research, email, etc. Except as provided in Section I (F) of this policy, all Internet shall be work related.

B. **Prohibited Uses of [redacted] Internet**. All internet use is traceable. No staff person should use program equipment for purposes prohibited by program policies or that could not be reasonably explained to persons outside the program. Employees are prohibited from viewing

material on any piece of [redacted] equipment that is pornographic in nature or in any use of the internet that violates civil or criminal law.

Use of peer to peer file sharing services (e.g., Bittorrent, etc.) while connected to any [redacted] network, or on any personal device that has [redacted] Sharepoint synced to it, is prohibited.

C. **Remote Work at Home**. If employees choose to use wifi on their home network, they must use a strong password (numbers, letters, symbols) of at least 6 characters and WPA2 encryption. The encryption key should not be shared with others outside the employee's household such as occasional visitors or friends. If your router only has WEP wifi security you should consider getting a new router because the password can easily be hacked by a neighbor or someone parked near your house.

D. **Remote Work away from Home**. If you plan to regularly work from a remote location other than your home, please ask [redacted]-IT to set up a VPN connection for you to use rather than using wi-fi connections at coffee shops, airports, hotels, or other places. Please give [redacted]-IT 72 hours notice to set it up and test before you need it for the first time.

III. USE OF PERSONAL DEVICES FOR [redacted] WORK

[redacted] is a hybrid work environment, meaning that many employees work remotely some of the time. It is [redacted]'s goal to obtain a [redacted] laptop for every employee working remotely, but until then, some employees will be working a significant amount of the time from a personal device. Once an employee has been assigned a [redacted] laptop, that is the device that is to be used for all work, both remote and in-office. In addition to the Equipment provisions of the [redacted] Remote Work Policy (Section C), the following rules apply to use of personal devices for [redacted] work:

A. All [redacted] employees are assigned a desktop or laptop computer (assigned device) that is adequate to perform their job duties. For this reason, generally and absent any temporary policy noting otherwise, personal devices are not permitted to be used at [redacted] offices absent a specific business case for doing so (such as a work need to use a program that is not available on a [redacted] device) and permission to do so from [redacted] IT. This applies to [redacted] employees and students.

B. The use of unprotected mobile devices to access or store confidential data is prohibited regardless of whether the equipment is owned or managed by [redacted] Every user of mobile devices must use reasonable care as outlined in this policy to protect against a confidential data breach.

C. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices used to access [redacted] systems must be protected by a password. Employees should use a password manager (such as Bitwarden) to protect and manage their [redacted] passwords and data. [redacted] Passwords and data should not be stored on a personal device (including phone) in an unsecured manner that can be retrieved if their device were lost or stolen.

D. Employees understand that their access and/or connection to [redacted] networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. [redacted] reserves the right to refuse the ability to connect

to [redacted] infrastructure if it feels such equipment is being used in a way that puts the program systems or data at risk.

E. In the event [redacted] confidential data is contained on any personally-owned computer or device that is lost or stolen (i.e., email, PIKA CMS, network share), it is the employee's responsibility to notify [redacted] or [redacted] IMMEDIATELY at [redacted]

F. Employees' access to company data is limited based on user profile and permissions defined by IT and automatically enforced.

G. Employees are required to apply multi-factor authentication to access [redacted]'s resources: email, calendars, contacts, documents, etc.

H. Staff must enroll their personal devices they wish to use for work purposes with Azure Active Directory before downloading Microsoft Office 365 desktop applications and syncing to [redacted]'s resources. Instructions for syncing can be found online (e.g., Enroll your personal Android device using the Microsoft Intune Company Portal; Enroll your personal macOS device using the Microsoft Intune Company Portal; Enroll your personal iOS device using the Microsoft Intune Company Portal; Enroll your personal Win 10 devices using the Microsoft Intune Company Portal).

I. Students and volunteers should not sync [redacted] data through OneDrive app, unless they have been given permission to work remotely.

J. [redacted] will remotely remove all [redacted]-related data from an employee's, student's, or volunteer's device when:
   a. The device is lost or stolen,
   b. The employee's employment is terminated,
   c. IT detects or learns of a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

K. [redacted] assumes no responsibility for repair, maintenance, or replacement of personally owned equipment used for remote work. [redacted]-IT may provide general guidance (i.e. working with staff to connect their devices to [redacted] printers) but will not troubleshoot connectivity issues or provide in depth assistance to personally owned equipment.

L. [redacted] reserves the right to revoke this privilege if users do not abide by these policies. Limited exceptions to policy may occur due to variations in devices and platforms.

IV. COMMUNICATION

A. Staff are responsible for checking and responding to voicemail and email messages at least daily. If you're not going to check voicemail or email messages for longer than three days, you should leave a message to that effect on your voicemail and email.

B. Staff should not make any communication using voicemail or email that shouldn't be made in a letter or memorandum. Each of these systems presents its own opportunities for humor.

However, sometimes things that seem funny at the time appear cruel or otherwise objectionable when received in an email or a voicemail message. Please be aware of this and try to avoid communications that may cause hurt feelings.

C. [redacted] email accounts are to be used for [redacted]-related correspondence. Employees shall not forward their [redacted] email to a personal or other email address. All [redacted] correspondence should be transmitted from and stored in your [redacted] email account only.

D. All email accounts should contain the following text below the signature:

This electronic communication may be subject to the attorney client privilege and may contain confidential information. If you are not the intended recipient, any distribution, copying or disclosure is strictly prohibited. If you have received this communication in error, please notify the sender immediately and delete this copy from your system. Thank you for your cooperation.

E. For staff who would like to text with clients, this should be done directly through our Case Management System (Pika or JusticeServer), RingCentral, or WhatsApp. If the client or attorney needs to text photographs or documents, this can be done via RingCentral. Email is a preferred method of client communication when available because text is not encrypted and also our governance of data in RingCentral is not as good as in the CMS, or Gmail, or SharePoint. Some offices may be given shared cell phones for using WhatsApp to obtain signatures and text with clients out of the country, for use as a mobile hotspot to connect to the internet when in the field, and for scanning and saving documents/pictures to Sharepoint. Employees should use their [redacted]-assigned phone number in all work-related communication. Employees are not required or expected to use their personal cell phones for work purposes, but if it is unavoidable, employees may apply for a phone stipend per the [redacted] Cell Phone policy.

F. Please refer to Section VII below for more information related to sharing confidential information electronically.

G. [redacted] currently supports several options for hosting video conferences with clients, co-workers, and partners: Google Hangouts; Teams; RingCentral; and Zoom (ask [redacted]-IT if you need login credentials to host a meeting). Zoom is the recommended platform for trainings and webinars. When recording a training or webinar on any platform, please be conscious of the length of the training, and how long the video needs to be stored. Zoom meetings/webinars should be recorded in the cloud, not locally, and due to limited storage, they should be deleted from Zoom when they are no longer needed. If you need to retain a recording indefinitely, please reach out to [redacted]-IT to discuss where to store it.

V. DATA STORAGE

A. **File Naming**. All staff should place case-related computer documents they work with in the appropriate common directories and subdirectories. When naming directories, subdirectories, and files, use only letters, numbers, dashes (-), or underscores (_); do not use brackets, parentheses, periods, or other characters; abbreviate whenever possible. Follow a single scheme in organizing your files in directories and subdirectories, and share your

scheme with your manager.

B. **File Storage Organization**. Over time, your directories will become full and this may make locating documents more time consuming. We suggest that you periodically (at least once a year) clean out your directories. This can be done by deleting files that are no longer relevant. It is probably a better practice to create a subdirectory for noncurrent materials e. g., G:\PS\OLD\. Any noncurrent documents (e.g., files relating to closed cases) can be moved to this subdirectory where they will be "out of the way", but can be retrieved in the future if they are needed for any reason.

C. **Common Directories**. When working in common directories you should never delete a file unless it was created by or for you, and even then use caution. Before you modify a document not created by or for you, copy it to a new file name in your directory.

D. **Backup and recovery**. Incremental backups are performed each night over WAN and LAN networks to a dedicated backup host with a full backup each weekend. Restore operations are tested at least quarterly. Only IT administrators have access to the backup server. If users notice missing directories or files, please notify [redacted] and [redacted] promptly at [redacted].

E. **Data storage in [redacted]'s CMS**. Staff are encouraged to paste or upload important client documents—litigation plans, substantive emails, substantive letters, substantive orders, etc.—into Pika or any future Case Management System (CMS).

VI. RESPONSE IN THE EVENT OF A DATA BREACH

A. **Definitions**.

1. "Data Breach" means the loss of control, compromise, authorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user access or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purposes.

2. "Personally Identifying Information (PII)" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

B. **Actions in the event of a data breach**. [redacted] stores personally identifiable information in staff email (currently Gmail), in our case management system (currently Pika), and in our

document storage system (currently Office 365/SharePoint) and Box (VERA only). In the event of an actual or imminent breach of personally identifiable information, [redacted] IT staff will take all reasonable measures to immediately stop and repair the actual or imminent breach.

C. **Notifications in the event of a data breach**.

1. In the event of a data breach, [redacted] will:
    a. notify the affected individual(s) without unreasonable delay, consistent with legitimate needs of law enforcement, or consistent with measures necessary to determine the scope of the breach and to restore the integrity of the data system;
    b. notify law enforcement of the breach as appropriate; and
    c. notify funders as required by the terms and conditions of the funding source.

2. [redacted] will include the following information when notifying the affected individual(s):
    a. That the individual's personal information was acquired or reasonably believed to be acquired by an unauthorized person;
    b. The date or dates of the breach or possible breach;
    c. Those elements of personal information that were likely acquired.

3. [redacted] may delay notification if a law enforcement agency requests a delay for criminal investigation purposes. Notification will be made after the law enforcement agency determines that it will not impede the investigation.

4. [redacted] will notify the affected individual(s) by one of the following methods:
    a. Written notice to the person's last known address in [redacted]'s records;
    b. Electronic notice consistent with applicable provisions of 15 U.S.C. 7001;
    c. Telephonic notice to the last known telephone number in [redacted]'s records; or
    d. Substitute notice, such as electronic mail, prominent posting on [redacted], or notification to applicable local or statewide media, if one of the following conditions exist:
        i. the cost of providing notice would exceed $250,000
        ii. the number of individuals to be notified exceeds 500,000; or [redacted] has insufficient contact information.

VII. CONFIDENTIALITY

A. **Passwords**. All employees are issued a username and password for their computer, SharePoint, Case Management System, email, and other miscellaneous systems. These passwords should not be shared and should be kept confidential. Employees should choose passwords that are at least eight characters long and contain a combination of uppercase and lowercase letters, numbers, punctuation marks and other special characters.

Employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective. Users should avoid dictionary words, common phrases and even names. Employees must choose unique passwords for [redacted] accounts, and should not use a password that they are already using for a personal account. If the security of a password is in doubt or if it appears that an unauthorized person has logged in to the account, contact [redacted] and [redacted] IMMEDIATELY at [redacted].

B. **Desktop PIN**. Do not ever change your desktop PIN. If you do have a need to set or change your desktop PIN and haven’t been assigned one by [redacted]-IT, please inform [redacted]-IT of your PIN as soon as possible so they can access your device.

C. **Common Files and Confidential Documents**. Any file on SharePoint may be accessed by anyone with access to that Site. Managers have separate Sites for management documents. Staff may not access management Sites without permission. If others find a need to have a Site with restricted user access, please contact [redacted]-IT.

D. [redacted]**’s Internal Website**. The information on the [redacted] internal website is [redacted] policies and guidance to assist staff in complying with these policies. These sites are password protected and their contents are confidential. The materials on [redacted] sites may not be used for any purpose except for [redacted] program purposes or shared outside of [redacted] without the prior written approval of a Director of [redacted] or [redacted]. Violation of this "terms of use" policy could result in employee discipline up to and including discharge.

E. **Email**. Email is confidential. You should not read other people's email without their permission.

VIII. SHARING AND COMMUNICATING CONFIDENTIAL CLIENT INFORMATION

Client information may only be shared electronically after the client has authorized the sharing of their information.

A. Internal and External Sharing of Confidential Client Information.

1. Whenever possible, sharing confidential client information internally or externally should be done using [redacted]'s secure data sharing platforms.

2. If a [redacted] employee is contributing confidential client data to a partner’s platform, SharePoint, Teams, or another secure platform is preferred.

3. If a [redacted] employee is sharing or communicating information that is not confidential (including non-confidential client information), that may be shared with internal or external partners via a less-secure platform such as Google Drive. Documents containing client information may not be shared via link or shared with a generic or group email address.

4. Currently, [redacted] supports SharePoint, Teams, and Box (MIRC only) as secure data sharing platforms.

5. External user organizations sharing confidential client information with [redacted] must sign a Data Sharing Agreement. [redacted] will make template Data Sharing Agreements available.

B. **Internal and External Communication of Confidential Information**.

1. All internal communication (i.e., communication between [redacted] employees) including confidential client information must be done using [redacted] email address. Anyone without a [redacted] email address is considered an external partner (including casual students or volunteers).

2. All communication (external and internal) that includes confidential client information must be encrypted. Some grants may also require all communication about certain cases or work to be encrypted.

3. All communication (internal and external) including confidential non-client information (including passwords, access codes, bank account or credit card information) must be encrypted.

4. Currently, [redacted] supports Virtru and Adobe Sign as encrypted options for email.

C. **Determining What Client Information is Confidential.**

1. "Personally Identifying Information (PII)" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

2. Similarly, the decision about what items of PII must remain confidential must be done on a case-by-case basis. Some information must remain confidential such as dates of birth, social security numbers, bank or credit card account numbers, medical records, tax records, drivers' license or ID numbers, and others. Other information is not as clear. The need for names, addresses, employment/employer information, and many other items of PII to remain confidential depends on the specific circumstances of the individual and the case. Advocates must make these decisions in each instance, and are encouraged to seek guidance from their managers as needed.

3. Advocates should also minimize sharing PII about clients whenever possible. When emailing, consider what information must be shared, and whether it's possible to

communicate without using PII or to share redacted documents when consulting or sharing pleadings.

D. **Use of SharePoint Sites and Teams for Sharing Data**

1. [redacted] staff can create SharePoint Sites and Teams groups for the purpose of sharing documents, but these may not be used to **permanently** store client confidential or case information, or as the **primary** place to store such information. Such information should be permanently stored in your office SharePoint sites (which are closed to external users).

2. Sites and Teams **can** be used for collaboration with internal or external partners on projects, and may be used to share confidential information with internal or external partners for the duration of the project. See the training and slides from [redacted] IT for more information on [redacted] staff use of Sharepoint Sites.

3. Staff can set up their own Sites or they can ask [redacted] IT for assistance.

4. External users, upon their first login, will be required to register a form of MFA (multi-factor authentication) with [redacted] to ensure that no unauthorized access is granted. Please see Instructions for External Users Accessing [redacted] SharePoint Sites and Teams.

5. Duration of sites - External SharePoint sites will be archived by [redacted] IT following a period of inactivity of 6 months. After a site is archived it won't be accessible by members but it won't be deleted. However, it should be reiterated that content that needs to be retained should be moved to permanent, internal SharePoint sites.

IX. OPEN SOURCE SOFTWARE

[redacted] supports the use and creation of open source software as generally in line with our values as a nonprofit poverty law program. We will endeavor to use, support and contribute to open source software in our program whenever feasible.

X. TECHNOLOGY PROJECTS AND PURCHASES

[redacted]-IT is dedicated to meeting the technology needs of the program in a consistent and efficient manner across the program, and are the program experts in technology solutions. Technology requests should be made in writing to your local office CRP and Managing Attorney, and requests for technology solutions to existing problems should be made to [redacted]-IT. Technology decisions are made on a program wide basis in accordance with the technology plan. Before implementing any new technology solution, staff must consult [redacted]-IT.

Technology purchases: Requests for purchasing any technology equipment (keyboards, cell phones, mice, recording equipment or programs, laptop sleeves, etc.) should not be done without consulting [redacted] IT first. [redacted] IT often has extra equipment available, and may also make recommendations for specific purchases to ensure compatibility with existing equipment, and that high quality equipment is available to staff and there is consistency and across the program for purposes of future maintenance. [redacted] IT may recommend a particular item to be purchased by the employee's office through Staples, or may purchase the item and have it shipped to the employee.

XI. REPORTING AND RESPONDING TO TECHNOLOGY

POLICY VIOLATIONS

Any violation of [redacted] technology policies should be reported to [redacted] immediately.

Violations of this policy constitute employee misconduct under the [redacted] CBA and may result in employee discipline, up to and including discharge. [redacted] reserves the right to restrict an individual's access to technology resources as a result of inappropriate use.

Updated September 2021

(signature page below)

AGREEMENT REGARDING TECHNOLOGY POLICY

I have read and I am familiar with the [redacted] Technology Policy, and I agree to abide by all terms of these policies. I also understand that [redacted]'s Technology Policy may be updated periodically, and it is my responsibility to be aware of changes made to the policy by reading emails related to the Technology Policy, and by periodically reviewing it on [redacted]'s internal policy website.

This signed acknowledgement must be submitted as part of your onboarding, and will be kept in your Personnel File maintained by [redacted] HR.

By: _____

Signed: _____

Dated: _____