2023 New York Statewide Civil Legal Aid Technology Conference

LSC Baselines

Wednesday, April 19, 2023
3:00 PM – 3:50 PM
Live Virtual Presentation
CLE Credits: 1.0 Practice Management

PRESENTERS

LSC Baselines | Practice Management CLE

Moderator: Ellen Samuel, Director of Consulting, Just-Tech

Speakers: Tony Lu, Senior Consultant, Just-Tech LLC; Jane Ribadeneyra, Program Analyst for Technology, Legal Services Corporation

Description: For the first time since 2015, The Legal Services Corporation is revising the technology baselines recommended to be in place within legal aid organizations. The presenters will share highlights about the baselines to help attendees understand the changing technology landscape and consider changes to improve their service delivery and operations

.

CLE RESOURCES

Legal Services Corporation Technology Baselines Public Comment March 2023

Legal Services Corporation Technology Baselines Public Comment March 2023

March 2023
For Public Comment

Legal Services Corporation
Technology Baselines

Technologies that Should Be in Place in a Legal Office Today

Version for Public Comment Period (March 2023)

LSC | America's Partner for Equal Justice

LEGAL SERVICES CORPORATION

Introduction

LSC is committed to developing a strategic vision for technology as part of its broader mission to enhance the quality of civil legal services across the United States. As a major part of that vision, LSC has defined the technology capacities that legal services organization should possess – or have available to them through a vendor or a partner – with publication of the Technologies That Should Be in Place in a Legal Aid Office Today (also referred to as the LSC Baselines). The original document was drafted at a 2006 LSC-led conference of technology experts from the private bar, foundations, the judiciary, academia, and LSC-funded programs. For subsequent updates – in 2015 and again this year – LSC has continued to seek feedback from a broad range of stakeholders across the justice community.

The technology capacities described in these Baselines are intended for any legal aid office that provides a full range of legal services, and LSC uses this document as a resource for its regular review of grantee program quality. The Baselines do not outline specific LSC grantee technology requirements, but are instead intended to provide helpful guidance to grantees and other legal aid offices on the use of technology to provide high-quality legal services to clients.

This draft revised version of the Baselines has been posted for Public Comment for 30 days from March 15, 2023 to April 14, 2023. Comments should be sent to techgrants@lsc.gov by April 14, 2023, with the subject line “LSC Technology Baselines.” LSC will then incorporate feedback from the public comment period and publish a final version in June 2023. Prior to publication, LSC will add applicable references to the LSC Act, LSC Regulations, LSC Performance Criteria, LSC Financial Guide, LSC Program Letters, and the ABA Standards for Provision of Civil Legal Aid. Additionally, the project team will update and incorporate useful websites, resources, and other tools for the broader access to justice, nonprofit, and technology communities.

Table of Contents

Summary of Significant Updates

Some of the major updates to the Baselines cover the significant changes in the way legal services are delivered because of the COVID-19 pandemic as well as the growth in cybersecurity threats since the Baselines were previously released in 2015, including remote/hybrid work environments, cloud computing and policies, new security baselines for networks and data, document management strategies, social media policy, and the use of web and video conferencing systems. The most significant updates are summarized by section below:

- **Overall Program Capacity**:
    - Programs should prioritize staff feedback on technology through the creation of a technology committee and conducting regular staff technology surveys.
    - Budgeting for technology must reflect the importance of implementing robust security practices and systems in the face of increased cybersecurity threats to legal aid organizations.
    - Programs should shift from on-premise data storage and servers to more reliable and accessible cloud-based solutions.
- **Sustainability**:
    - Budgeting for technology projects should reflect ongoing maintenance costs. Considerations for related budgeting and planning are provided.
- **Remote/Hybrid Work – Policies and Procedures**:
    - Programs must evaluate the lessons learned from the COVID-19 pandemic and develop a policy to account for remote work and hybrid (e.g., remote/on-site) service delivery models.
- **Management of Client and Case Data - Case Management System**:
    - Multi-Factor Authentication ("MFA") should be enabled across all systems, where applicable, especially on critical applications, such as a case management system to protect client information or utilize a single sign-on service ("SSO") / identity management solution that integrates cloud-based services under one MFA system.
- **Production and Supervision of Legal Work - Case Management System & Document Production**:
    - Programs should deploy technology, develop policies, and train staff on how to effectively provide legal services and supervise remote work in a fully remote and hybrid remote/onsite context.
- **Intake and Telephone Advice - Telephone Systems**:
    - Programs should adopt hosted telephone systems as their telephone solutions, to permit advanced functionality, provide more security, reduce administrative overhead, and make remote work possible.
- **Production and Supervision of Legal Work – Document Management**:
    - Programs should have a centralized approach for document management. New baselines and considerations were added to address the need for improvement in document management across an organization.
    - Programs may need to evaluate the need for a document management system ("DMS"), which can provide organizations with tools to better organize and search data, reduce

duplication of files, comply with retention policies, and provide tools to automate processes and electronic forms.

- **Advanced Editing for Appellate Brief and Major Litigation:**
  - New section added with baselines and considerations regarding essential technology tools, training, and software needed to conduct large projects, such as appellate briefs and major litigation.
- **Security:**
  - This section includes new additions and updated baseline recommendations regarding Security Policies & Procedures, Multi-Factor Authentication ("MFA"), Cloud Computing and Policies, Password Management, Mobile Equipment for Staff Use, Mobile Device Management, Security Awareness Training, Disaster Recovery Plan, Incident Response Plan, Endpoint Detection and Response ("EDR"), Email Security, and Cyber Insurance.
- **Legal Information for Low-Income Persons:**
  - This section was revised to provide updated baselines and considerations on providing legal information via websites and social media, including WCAG standards and triaging to help users identify their legal issues or effectively routing users when needed.
  - Programs should provide and use appropriate tools and technologies that meet the needs of relevant client populations and contribute to addressing the digital divide.
- **Communication and Collaboration**:
  - Programs should streamline their applications in use for collaboration by establishing standard collaboration tools organization-wide and developing clear internal policies for staff.
  - Programs should develop and use collaborative work environment tools (e.g., Microsoft Teams and Word Online) and should encourage real-time collaboration among staff.
- **Training and Technology**
  - This section has been updated for programs to ensure adequate internal capacity or outsourced support to provide onboarding and ongoing technology-related training. New important considerations have been added to assist programs with conducting training and developing training materials.
- **Administration:**
  - This section has been revised to include ticketing systems and communication strategies on after-hours support, essential HRIS software and functionalities, and updates to accounting functions.
- **Development/Fundraising**:
  - The Fundraising and Marketing section has new important considerations around Customer Relationship Management ("CRM") systems and revised needed capacities and functions for fundraising and marketing management.

1 Overall Program Capacity

1.1 Baseline for Overall Program Capacity – Planning

Needed capacities or functions

- Technology planning should be ongoing and integrated into the overall planning of the program for effective service delivery.
- Technology planning should include an assessment of the program's current needs and capacities to effectively position the program to incorporate new technological advances as they evolve.
- Technology plans should be reviewed and updated as needed every year.
- Technology plans should include measures to increase staff input and engagement in improving technology use, such as forming a technology committee and regularly using staff technology surveys.

Important Considerations and Best Practices

Technology should serve the mission and vision of the legal aid program (ABA Civil Standards, Standards 2.1 and 2.2.). As part of strategic planning, the program should consider how technology can be used to respond to the most significant issues faced by the communities it serves.

As part of technology planning, programs should consider periodically (e.g., every 3-5 years) engaging an independent technology consultant, with expertise with nonprofit and/or legal services organizations, to audit their technology systems and recommend improvements that promote efficiency, effectiveness, and optimize performance. An independent consultant can help an organization understand the value and importance of technology upgrades and the return on investment through greater efficiency and performance.

Programs should consider forming a technology committee with representatives from various staff levels and departments (e.g., management, case handlers, intake staff, etc.) to periodically review and assess program-wide use of technology and to help plan future enhancements.

For increasing staff input and engagement in improving technology use, programs should conduct regular technology surveys of their staff to gather feedback on technology, training needs, and pain points.

1.2 Baseline for Overall Program Capacity – Budgeting

Needed capacities or functions

Adequate funds should be budgeted by the Board of Directors for:

1. the ongoing maintenance and upgrading of hardware and software;
2. cloud-based systems, integration, identity management, security, and backup;
3. security-related expenditures, such as data and security recovery services, email security, cybersecurity training (see Security section);
4. the personnel/consultants necessary to manage, support, maintain, and secure systems and endpoints;
5. adequate support for remote and/or mobile work and supervision; and

6. ongoing trainings on the use of existing and new technologies.

Technology costs should be included in the budget of every project, program, and initiative. Organizations should work with funders to ensure that new initiatives include sufficient funding for technology.

Important Considerations and Best Practices

The organization should develop a plan as to how it will fund necessary technologies.

Replacing equipment on a consistent cycle vastly improves efficiency, support, budgeting, and planning. Organizations should maintain a clear equipment lifecycle policy or workstation replacement plan to inform the hardware planning process and to replace or upgrade equipment in the future.

Additionally, organizations should consider standardizing the equipment being purchased and creating an IT Capital Budget to ensure budgeting and planning is in place for new equipment. Budgeting should also include other equipment, such as servers, printers, scanners, docking stations, monitors, etc.

1.3 Baseline for Overall Program Capacity – Personnel

Needed capacities or functions

- An organization should aim for a ratio of approximately 1 full-time IT Support staff person (or equivalent) for every 50 employees. For larger organizations, this may include a combination of systems administrator(s) and Helpdesk IT associates.
- Ensure that personnel planning includes capacity for management-level technology leadership and strategy.
- Have sufficient technology staff or equivalent consultant or managed services capacity to:
    - Maintain and upgrade equipment and networks, as needed;
    - Secure, monitor and maintain all information systems, including cloud-based information systems, containing confidential program, personnel or client data;
    - Support and train program staff in the use of equipment and technology tools;
    - Develop and maintain knowledge of best practices in technology security, nonprofit purchasing options, and general technology best practices; and contribute to creating policies that are aligned with best practices and the organization's needs.
- Whether technology administration capacity is maintained internally or outsourced, the organization should plan for continuity of services in the event of loss or unavailability of staff.
- Adequate staffing or consultant time to maintain or contribute content to the statewide website and any program website.

Important Considerations and Best Practices

Organizations should also consider capacity for additional technology roles such as data analysis and management, knowledge management, and special projects management that require different knowledge and skills than systems administration and technical support.

Having adequate personnel does not necessarily mean having permanent and paid staff. Implementation, maintenance, and support of technological capacities can be outsourced to a professional organization, managed service provider ("MSP"), or to a legal services organization that

takes on such a role on a statewide, regional, or national basis. Virtual Chief Information Officer ("V-CIO") services are also available to provide outsourced strategic leadership capacity. When utilizing outsourced IT resources, the organization may still find it requires some on-site IT capacity to address issues that cannot be resolved remotely.

An important ingredient of having sustainable, effective technology that furthers a program's mission is the support of upper-level management. Without support from senior management, many technology strategies will fail. Support should include a demonstrated willingness to stand behind the integration of technology into program operations, and budgeting appropriate expenditures for technology support and staff training.

2 Sustainability

2.1 Baseline for Sustainability – Planning

Needed capacities or functions

- Have a strategy for ongoing maintenance costs on every technology project.

Important Considerations and Best Practices

- At the onset of project planning for new technologies or systems, it is important to consider the upkeep costs and any additional costs from integrations and customizations (e.g., integrating two systems requires additional administrative time and capacity).
- Prior to deciding on add-on applications and custom solutions, organizations should consider long-term sustainability and feasibility based on administrative capacity.
- Programs should consider long-term ownership and roles/responsibilities, including:
    - who is handling upkeep;
    - what upkeep is expected;
    - what needs to be documented during the implementation to make upkeep easier; and
    - how will new requests for changes be handled once the project is considered closed.
- Maintenance costs for custom development may increase the total cost of the project.

3 Remote/Hybrid Work

3.1 Baseline for Remote/Hybrid Work – Remote Work Policy

Needed capacities or functions

Have a remote work policy in place when offering remote or hybrid options for staff. The policy should define the following:

- purpose for the remote work policy and benefits;
- what remote work looks like for the organization;
- what technology is offered to support the remote work;
- contact for who can answer any questions about resources and information;

- if remote work stipends or equipment will be offered;
- contact for technical issues;
- core hours and working hours; and
- home base location and temporary work location protocols.

Important Considerations and Best Practices

The organization should determine how to develop its remote work policy and whether to incorporate cybersecurity elements. Some organizations may opt to have more standalone security policies or to combine cybersecurity elements into a comprehensive manual. See Security Policies and Procedures section. section.

Periodic reviews should be performed to ensure the remote work policy remains applicable as new technologies and practices are adopted and deployed.

4 Management of Client and Case Data

4.1 Baseline for Management of Client and Case Data – Case Management System (CMS)

Needed capacities or functions

The following capacities, including reporting features and access to client and case data, should be available:

- The CMS should offer the ability for organizations to:
    - Require multi-factor authentication ("MFA") for administrators and users to gain access to the system or use related technologies, such as single sign on ("SSO") identity management that requires multi-factor authentication;
    - Securely store and routinely back up data in standardized data formats;
    - Accommodate extraction of all stored data as needed;
    - Customize data entry processes to align with organizational practices and eligibility screening requirements;
    - Customize CMS displays, features, and processes to align with organizational needs, such as modifying field values and creating new fields;
    - Conduct timely conflict checks for both clients and adverse parties;
    - Enter and edit CMS data in real time, including for timekeeping purposes;
    - Securely and ethically transfer client and case data electronically to and from other service providers, provided that they have the appropriate technologies;
    - Perform routine case management functions remotely and securely;
    - Generate reports and extract case and client data (consistent with applicable privilege and ethical considerations) for strategic planning, program evaluation, reporting to LSC and other funders, responding to LSC requests for information, and other purposes;
    - Export case and client data in customizable formats in a manner that facilitates case work, such as document templates or summary screens;

- Assign appropriate funding sources to cases and activity records;
- Have the technological capacity to check for data integrity, ideally in an automated way (which ensures that integrity checks are performed regularly and uniformly), to reduce staff time and the risk of human error; and
- Have the capacity to integrate and securely share data with external systems to enhance and increase functionality, particularly in the areas of improved reporting, data analysis and visualization, document management, and integration with coordinated intake systems.

Important Considerations and Best Practices

- Organizations should consider technologies or capabilities to effectively transfer client and case data electronically to and from other service providers that can facilitate faster referrals and reduce the need for repetitive data entry.
- Aggregated case and client data can be a source of insight into patterns of issues facing low-income communities and can be useful to program planning.
- Ethical obligations require conflict checks.
- Consider configuring the CMS system to customize permissions and access differently depending on user groups (e.g., supervisors, report runners, pro bono volunteers, etc.)

4.2 Baseline for Management of Client and Case Data – Document Management

Needed capacities or functions

- Establish organizational standards and develop internal policies (e.g., procedures on storing, naming, and collaborating on files) that will contribute to more unified document management practices.
- Reduce the number of places where staff can store and manage documents, to improve ease of use and the ability to search for files easily.
- Determine where types of files (e.g., drafts vs. work product) should be stored in, include clear governance in internal policies, and consider methods for auditing compliance with this policy.

Important Considerations and Best Practices

Organizations should assess whether a Document Management System ("DMS") would meet its needs for a solution to centralize document management storage.

A DMS can be one of the most critical tools at play in the effective delivery of legal services. DMS platforms can provide organizations with tools to better organize and search data, reduce duplication of files, ensure continuity of services in the event of staff absence or loss, control versioning, and provide tools to automate processes and electronic forms. A DMS should integrate with or simultaneously support the organization's case management system and promote organization-wide collaboration.

5 Production and Supervision of Legal Work

5.1 Baseline for Production and Supervision of Legal Work – Case Management System (CMS)

Needed capacities or functions

- The CMS should offer the ability for organizations to:
    - Record case notes electronically including facts, advice, and services offered, with deadlines;
    - Store, or facilitate easy access to, case-related documents;
    - Record, edit, and view all case and client data needed throughout the lifecycle of a case;
    - Generate simple forms and letters, populated with relevant case and client data from the CMS;
    - Allow users to record their time accurately and contemporaneously, as needed;
    - Generate reports and extract meaningful data for case planning and organizational planning;
    - Provide remote access to the system, including databases as needed;
    - Strategically use the CMS to expedite and optimize intake and case management processes, such as phone routing, online intake triaging, securely exchanging data with partner online intake tools, and future compatibility with electronic filing systems; and
    - Facilitate ongoing supervision, including through reports and custom displays for supervisors.

Important Considerations and Best Practices

- Organizations should consider having a dedicated person/s responsible for managing the maintenance and upkeep of the CMS and policies for modifying the CMS (e.g., who decides what to change, how are changes communicated to users, how are changes tested/rolled out, how are changes documented).
- Offer documentation/resources and ongoing trainings for both new and existing users to make sure there is clarity on how to use the CMS and organizational expectations for CMS usage.
- Many features of case management software rely on consistent use by everyone in the office. Remote supervision, for instance, cannot readily be accomplished unless the case handler being supervised has entered information into the system for remote review. Group calendaring depends upon full use of the system. Full utilization, however, requires training and support and that the advocates using the system understand and experience the benefits of the system.
- An organization may need to consider Intake Process Improvement, Business Process Analysis, or similar projects with an independent technology consultant, if internal capacity is not available, to develop its strategy on using the CMS to facilitate and expedite the intake process.
- Organizations may seek funding needed to assess, optimize, and standardize its intake process while leveraging technologies to better serve clients and support advocates and program operations.
- Consider integrating the CMS with third-party tools and sites to reduce duplicative data entry, facilitate more efficient practices, and consolidate displays of information stored in different locations.

- See ABA Standard 5.5 on Case Files

5.2 Baseline for Production and Supervision of Legal Work – Calendaring

Needed capacities or functions

- Program-wide electronic calendaring system.
- A calendaring function for deadlines and appointments that can be viewed by appropriate staff.

Important Considerations and Best Practices

The program-wide calendaring system is intended to provide calendaring for program events, not for each individual's appointments, which should be separately available through an electronic calendaring function. However, court and other important dates should be on a shared calendar, whether program-wide or office-wide.

Organizations should establish a calendaring policy that defines staff responsibility in the upkeep and accuracy of case deadlines, other key dates, and staff availability.

See ABA Standard 2.2 on Effective Leadership

5.3 Baseline for Production and Supervision of Legal Work – Document production, document assembly, document templates

Needed capacities or functions

- An organization should leverage its case management system ("CMS") for document assembly or document template features to reduce duplicative data entry, such as retyping client information that has been entered in the CMS into common legal forms.
- Effective use of modern, cloud-based productivity software such as word processing, spreadsheets, and presentation software and training on their use.
- Develop a strategy to automate letters, retainers, forms, and pleadings that staff and pro bono advocates use routinely that includes management of forms from a central location, with a system to ensure that forms and pleadings are updated for legal sufficiency.
- Staff should receive training in the use of the automated documents.
- Capability for electronic filing of pleadings when required or allowed by court systems, including the ability to convert word processing documents into formats such as PDF/A (where required).
- Capability to capture electronic signatures where accepted.

Important Considerations and Best Practices

Several factors affect the degree to which document assembly software is useful to advocates and is used by them, including the following:

- Advocates must be fully trained in its use; and
- The content needs to be accurate and kept up-to-date and responsive to the needs of the advocate in serving clients.

This baseline envisions that legal aid programs will have internal capacity to develop basic templates that can be entirely completed with information from a case management system, such as name and

address of parties. These should include letters, retainers, and some common form pleadings. More mature programs may continue to develop more advanced templates that include conditional logic.

When commercial tools are available and suitable for use by legal aid programs, consider as part of document assembly the effective use of substantive law software. For example, legal aid programs may subscribe to dedicated packages for family law, bankruptcy, and estate law planning which are available as commercial tools in many states.

When implementing electronic signatures, review whether location related data is attached to the signature and whether they may be configured to reveal less specific information about the signer or turned off entirely to protect clients and staff.

5.4 Baseline for Production and Supervision of Legal Work – Advanced Editing for Appellate Brief and Major Litigation

Needed capacities or functions

- Train staff and provide technology tools to assist staff in working collaboratively on the production of large projects, such as appellate briefs and major litigation.
- Provide tools that allow staff to simultaneously edit and maintain a version history of collaboratively produced documents.
- Provide PDF editing software to add and remove pages, automatically redact sensitive information, rearrange pages, and add running headers and footers (e.g., Bates numbering)
- Staff who work on appellate briefs should have tools to produce tables of contents, tables of authorities, and to maintain citations.
- Staff should have an electronic method to organize discovery. This should include the ability to tag, add Bates stamps, and to find relevant discovery responses.

Important Considerations and Best Practices

- Organizations that handle large litigation cases or appeals should have tools to effectively produce briefs and manage litigation that requires sifting through discovery.
- Modern operating systems like Windows and Apple OS could generate PDFs natively.
- Microsoft Office has basic features to manage citations, but commercial tools and free tools, such as Zotero, have additional features that improve ease of use.
- Commercial tools, including Lexis for Microsoft Office, can automatically recognize citations and generate a table of authorities when required by local rules.
- Document management platforms have powerful features for managing discovery, but even basic cloud document tools such as Microsoft's OneDrive and SharePoint support tagging and finding text inside a large document library.
- Examples of PDF software that can handle brief production needs include: Adobe, Nuance PDF Converter Pro, Foxit PDF Reader, and PDF Xchange Pro.

5.5 Baseline for Production and Supervision of Legal Work – Timekeeping

Needed capacities or functions

- Electronic timekeeping is available and utilized.

- Electronic timekeeping systems can integrate with other key systems such as payroll or human resources systems.

5.6 Baseline for Production and Supervision of Legal Work – Supervision

Needed capacities or functions

- Data to support the supervision of legal work, including case lists and activity, are available to supervisors and management.
- As necessary, remote access to case files for review by supervisors.

Important Considerations and Best Practices

Consider using the data from a case management system to develop real-time reports and data dashboards to improve the ability of supervisors to monitor legal work.

Implementation of a document management system ("DMS") can significantly enhance the ability of a supervisor to access and review case files. While integrating a DMS with a case management system will yield significant efficiencies in case and document management, utilizing a DMS along-side a case management system ("CMS") still has significant benefits over a standard network file-share system, including automatic document versioning, use of metadata to manage files, and the ability to index and search the contents of all documents.

See ABA Standard 6.5 on Review of Representation

5.7 Baseline for Production and Supervision of Legal Work – Online legal research

Needed capacities or functions

- Online tools for conducting legal research using up-to-date primary sources, including laws, regulations and cases, available from every advocate's computer with staff training regarding its use.
- Access to statewide materials, including forms and pleadings, legal education materials, brief banks, and topical email lists.

Important Considerations and Best Practices

See ABA Standard 6.7 on Providing Adequate Resources for Research and Investigation

6 Records Management

6.1 Baseline for Records Management – Electronic Records

Needed capacities or functions

- Filing of all electronic records, retaining them in accordance with the program's defined retention policies, assuring their accessibility and properly disposing of them when appropriate. Potential records in question include:
    - All data files across systems (e.g., accounting, case management, grants management);

    - Electronic case-related documents;
    - Email messages;
    - Instant messaging (where used); and
    - Transcribed or recorded telephone messages and conversations.
- Policies that govern permissions or access rights to electronic files, including the right to view, edit, move or rename files. An organization should grant access to folders and cases on an as-needed basis (e.g., by area of work) to protect client privacy, reduce the risk of accidental data leaks, and reduce the damage from potential ransomware attacks.
- Policies that clearly define the correct repositories in which each type of electronic record must be kept, as well as procedures to review and audit repositories and records for compliance.
- For LSC grantees, the records management system must be compliant with LSC and all other legal requirements in the maintenance of records, including the confidentiality of client records and access for LSC reporting and reviews.

Important Considerations and Best Practices

- As a best practice, organizations should apply permissions based on the principle of least privilege ("PoLP"), which is an information security concept that means a user should only have access to the specific data, resources, and applications needed to complete required tasks.
- Records management should be undertaken with an awareness of the growing convergence between records management (all records), case management (data associated with a case or matter) and knowledge management (specific content that needs to be identified and made accessible on demand)
- SMS messaging is an increasingly important means of interacting about legal work in law offices and may involve information and analysis relevant to a case. Such messages that contain case-related information need to be made a part of the electronic case file. Organizations should develop a governance policy that helps case handlers determine when such messages need to be made a part of the electronic case file and ensure that case-related information is streamlined to the case management system ("CMS"), if SMS messaging is not already integrated with the CMS.
- Document management systems ("DMS") can significantly improve an organization's ability to monitor and enforce record retention policies through document auditing features, reporting, and metadata analysis.

7 Knowledge Management

7.1 Baseline for Knowledge Management – Pleading and brief banks, and other electronically stored data and information

Needed capacities or functions

- Store and retrieve sample pleadings, briefs, motions, and other documents based on content.
- Program staff use an effective method for finding documents by search or logical browsing and can purge documents. Findability may be based on a document management system or content-searchable email lists, wikis, or shared folders.

- Electronic access to internal forms and procedures.
- Program-wide accessible and searchable contacts management system.
- Electronic access to practice guides.

Important Considerations and Best Practices

Effective knowledge management requires adequate staff time to identify appropriate content for inclusion in the system and to tag it appropriately for easy accessibility. Staff who produce the materials that become part of the knowledge to be made available need to be committed to identifying and submitting documents, such as briefs and pleadings. To that end, there should be appropriate training and visible support for the system from the program's senior management. Dedicated staff capacity to develop and maintain the information architecture may be required to ensure continued effectiveness of a knowledge bank over time.

A well-designed intranet can serve as a solid foundation for all knowledge management needs in the organization. Care should be taken to properly design the information architecture of the intranet and identify responsibility for its upkeep.

Consider how technology can be used to institutionalize knowledge of key employees (e.g., what they know, what they do, specialized skills, etc.)

Programs may use the contacts management system to store information on contacts, such as pro bono and PAI attorneys, courts, judges, and adversarial counsel.

8 Intake and Telephonic Advice

8.1 Baseline for Intake and Telephonic Advice – Telephone Systems

Needed capacities or functions

- Implement a hosted phone system across the entire organization.
- Monitor call volume and craft a strategy as to how it will address issues around excess demand to provide information over the phone to callers.
- Call routing by language, substantive and/or geographic area.
- Ability to serve persons with speaking or hearing disabilities through access to TTY, Video Relay Service ("VRS"), or Video Remote Interpreting ("VRI").
- Technology to review busy signals, wait times, dropped calls, etc.
- If the program does telephone call backs, it should look at technology systems that facilitate an efficient callback system.
- Provide recorded information to callers while waiting on hold or after hours.
- General intake should consider online intake as well as more traditional means of application for services.

Important Considerations and Best Practices

- Hosted phone systems are becoming standard among more legal aid organizations and provide the following capabilities and benefits:

    - Monitoring and reporting features that would allow for call data analysis (e.g., determining resource allocation based on call volume by office or identifying at what points callers hang up to improve call flow);
    - Access to translator services or auto-attendant messages that can cover primary languages based on client base;
    - Advanced functionality and scalability, especially for call center needs;
    - Less infrastructure needed onsite to maintain and support;
    - Redundancy and backups done by the provider;
    - Upgrades to features and functions are done as they are released;
    - By default, most hosted solutions allow you to use the system from a physical desk phone, desktop client, web browser and smartphone; and
    - More security protocols.
    - Less time spent by IT resources to manage an on-premise phone system.
- Legal aid law offices that use SMS through a hosted phone system, should develop a governance policy to ensure that case-related information is streamlined to the case management system ("CMS").
- Telephone systems should be designed to meet the needs of relevant client populations. This includes language proficiency and sensory impairment issues, as well as consideration of difficulties seniors may have with auto-mated attendant systems, the cultural differences that may deter new immigrants from understanding automated advice, etc.

8.2 Baseline for Intake and Telephonic Advice – Electronic desk manual

Needed capacities or functions

Programs should have an electronic desk manual that serves as a guide for intake workers to provide appropriate information, advice, or referral and meets the following criteria:

- Readily available;
- Centrally located;
- Easily searchable; and
- Easily updated.

Important Considerations and Best Practices

- This could be built into a case management system, document management system, central knowledge base or be available on a shared drive.
- Consider use of a knowledge management or document management system for its ease of access and administration and searchability.

9 Legal Information for Low-Income Persons

9.1 Baseline for Legal Information for Low-Income Persons – Legal Information via Websites and Social Media

Needed capacities or functions

Programs should collaborate in providing a statewide website with the following features:

- Current information regarding legal services programs and their services;
- Relevant and up-to-date self-help material, legal information, and referral resources presented in plain language;
- Capacity to properly serve persons with limited English proficiency;
- Modern visual and interaction design components that enhance usability and match users' expectations of current web-based experiences.
- Website designed and maintained in compliance with accessibility principles outlined in Section 508/WCAG 2.0 AA; and
- LSC programs' participation in the website is in compliance with LSC restrictions.

In addition to general legal information available on a statewide website, the organization itself should have a compelling web presence that includes:

- Description of what services the program offers;
- Links to available triage systems, online intake, and help lines;
- How to contact the program; and
- How to apply for services.

Important Considerations and Best Practices

To assist users in identifying their legal issues and finding the most suitable legal help, it is highly recommended that programs integrate legal triage systems into their statewide websites. These triaging experiences can guide users to the appropriate resources and providers that can address their legal needs effectively.

Programs should adopt content maintenance protocols that outline how the justice community will periodically review content for accuracy, plain language, and overall usability.

To the extent possible, a program should be certain that the content of websites to which it refers people is accurate and up to date. For frequently used websites, it may wish to confirm that the website has quality control measures and spot check the contents.

Pleadings and other forms for use by self-represented litigants should be developed as much as possible through a collaborative process with the courts in which they will be used, along with other legal services programs and justice community stakeholders.

If an organization intends to leverage social media for outreach or legal information, it must create a clear policy that governs its proper use. The policy should specify roles and provide guidelines for content and branding across different social media platforms, and ensure that permissions are up to date.

9.2 Baseline for Legal Information for Low-Income Persons – Addressing the Digital Divide

Needed capacities or functions

- Ensure all websites are mobile-responsive, in order to provide information to clients who use mobile devices;
- Utilize technology features to send reminders or alerts to clients of important dates or deadlines or in formats that the client community is likely to use;
- Provide clients access to video-conferencing tools when needed;
- For organizations working with rural populations, laptops, tablets, mobile workstations, wireless printers, and mobile hotspots may be needed for clients to make calls and use the internet.

Important Considerations and Best Practices

The digital divide is generally defined as the gap between individuals or communities that have access to technologies (e.g., internet or digital devices) and those that do not. Organizations should be aware of how the digital divide is a problem in legal aid since it has created significant barriers to client populations that need legal services but lack the necessary technology or digital skills. This baseline envisions that legal aid programs will plan for the appropriate tools or formats to best serve client populations that are particularly affected, such as rural or remote communities, and contribute to addressing the digital divide.

During the COVID-19 pandemic, when courts were forced to implement online hearings, lack of access to video conferencing technology became a significant barrier for low-income litigants. Legal aid organizations should have the capacity to create private video conferencing stations for clients to attend remote hearings, for courts that continue to hold such hearings or in the event that they become necessary and widespread again.

Adopting new technologies to make service delivery more efficient can sometimes have the paradoxical effect of making it harder for certain populations to access legal services. For example, a push to funnel intakes through an online intake site to make intake workflows more efficient can create barriers to those without broadband internet access or with limited English proficiency. Organizations implementing new client-facing technologies should ensure that service delivery is still designed with those who have the least amount of access to technology in mind.

Information websites must be designed using a mobile-first design principle, for easy access by, and interaction with, mobile devices by providing information in smaller, simplified sections that are readable on a smartphone screen. Mobile-responsive web design is now a standard in the web development industry.

Studies have shown that read and response rates on SMS text messaging are significantly higher than other platforms, including email, making this technology critical to an organization's mobile strategy. Generally, SMS should be a feature within a case management system (see Case Management System section).

9.3 Baseline for Legal Information for Low Income Persons – Community legal education

Needed capacities or functions

Community legal education presentations are supported by effective use of technology, such as online conferencing, videos, and other appropriate technologies.

Important Considerations and Best Practices

Care must be taken to ensure that any technology-enabled community legal education projects are designed to enable easy access to the presentation. Workflows or systems that require users to register using an email address or enter a password may create significant barriers for users.

See ABA Standard 4.3 on Participation in Statewide and Regional Systems

10 Support for Use of Private Attorneys

10.1 Baseline for Support for Use of Private Attorneys – Support for program efforts to accept, refer and track pro bono and PAI cases

Needed capacities or functions

Programs should have the following technology in place to support their pro bono and PAI programs:

- A website that may include such features as allowing pro bono lawyers and other case handlers to review available cases and volunteer, posting of training and resource materials, and calendars of training opportunities;
- A case management system that will track referred cases, time spent on those cases and work accomplished, and automate oversight of pro bono and PAI cases to promote timely case closure;
- A volunteer management system that will track a volunteer's history with the organization, including participation in clinics, acceptance of pro bono cases, and financial support to the organization; and
- A strategy to share client and case data securely with volunteers using electronic means.

Important Considerations and Best Practices

Case management systems may provide the ability to create a website that features pro bono opportunities directly drawn from the case management system. Also, consider whether regional or statewide pro bono opportunities sites or platforms exist that may be leveraged.

When developing a pro bono opportunity website, consider whether the site will require a password to view opportunities. Requiring a password may provide better information and serve as a stronger signal of the potential volunteer's interest but may also be a prohibitive barrier that discourages many potential volunteers.

When considering volunteer-facing technology, combining the case opportunity, training and resource materials, and calendars on one website is preferable to minimize confusion for the volunteers, and

make it easier to advertise, maintain and manage. Designate who is responsible for which section and how often the pages/resources/materials will be reviewed and updated.

When creating or updating new technology resources, it is best practice to perform user-testing with volunteers who are the target end-users.

Consider using a specialized Customer Relationship Management ("CRM") system to manage information about volunteers. System's such as Raiser's Edge and Neon-CRM, which were developed for donor relationship management, have volunteer-management capabilities, and combining donor and volunteer data can provide significant benefits to both resource and volunteer development.

10.2 Baseline for Support for Use of Private Attorneys – Direct support for volunteer attorneys and other volunteer case handlers

Needed capacities or functions

- The program provides assistance and support in pro bono and PAI representation, which may include automated documents, pleadings and brief banks.
- The program provides volunteer attorneys and other case handlers with training and resource materials through the use of technology, such as web conferencing, video conferencing and hosted online trainings.
- One way to provide these resources for volunteers would be to use a statewide website section dedicated to support for private attorneys and other case handlers.

Important Considerations and Best Practices

The extent to which private attorneys and others can avail themselves of technologically supported assistance is obviously a function of the degree to which they have technological capacity to do so, a factor that varies considerably by location and size of office.

When deploying training and resource materials, consider whether the information needs to be kept in a system that requires a password. It may be more important to remove all barriers to participating in the pro bono opportunity to increase engagement.

11 Security

11.1 Baseline for Security – Policies and Procedures

Needed capacities or functions

- The organization should develop policies to ensure secure remote practices. Ultimately, an organization should determine how to develop, update, or expand upon its policies.
- Policies may be standalone or in a comprehensive manual but should include the following security elements (see additional information in LSNTAP's Security Toolkit: Security Policies):
    - Acceptable Use Policy;
    - Remote Access Policy;
    - Data Classification;
    - Data Retention;
    - Physical Security;

    - Strong Password Requirements;
    - Disaster Recovery Plan (see Disaster Recovery Plan section);
    - Security breach and incident response (see Incident Response Plan); and
    - Policies on organization-owned equipment or Bring Your Own Device ("BYOD"), if applicable (see Mobile for Staff Use section).
- Periodic reviews, at least once a year, should be performed to ensure policies remain applicable as new technologies and security practices are adopted and deployed.
- Operating systems, antivirus software, and other software applications should have the most current patches and definition updates and remain patched on a regular cycle.
- Routinely maintain backup and recovery systems pursuant to grant assurances, including off-site backups.
- Any additional security policies and procedures for protecting client and case data, sensitive personal and personnel data, and all communications from loss or unauthorized intrusion.
- IT equipment should be kept in a secure environment with appropriate ventilation and cooling.
- IT should enable logging/auditing to be able to monitor changes made in the environment and by whom.

Important Considerations and Best Practices

A legal aid organization has a significant amount of confidential information, both about its clients and its operations. A lot of client and operational data is stored electronically, and the risk of outside intrusion into the program's network increases as does the potential damage of such an intrusion. There are a variety of potential risks:

- Direct hacking into the program's network;
- Potential loss or improper access to portable technology, such as laptops, tablets, mobile phones, and flash drives; and
- Inappropriate use of the web by staff who may access high-risk websites, exposing the firm to malicious software.

A program should have policies, procedures and systems in place to help avoid such losses.

An organization may want to consider developing a comprehensive technology security policy and procedures manual that enumerates all of the organization's policies on technology use, data repositories, data-loss prevention, and disaster recovery procedures, etc.

While every organization may vary in its technology security standards and practices depending on organizational size, structure, infrastructure, and resources, it is essential that every organization identifies some standards and practices by which it will measure its security readiness. Consider adopting a well-known, industry-recognized security and compliance standard, such as the HIPAA-compliant HICP standard for small businesses (Learn more here).

There are several existing resources available to help quickly and inexpensively develop a set of customized policies that are a good fit for the organization.

An organization may want to leverage an internal technology committee or its board members as additional resources since policy development can be a significant undertaking.

In the event of a disaster or significant systems outage, organizations may want to consider printing out policies to ensure they will still be accessible.

It is possible to outsource some responsibility for assuring the security level of a provider's information technology and communication system is adequate. Programs should consider having an outside firm conduct a security audit every year and/or work with outside experts on an ongoing basis to ensure an acceptable security posture.

11.2 Baseline for Security – Multi-Factor Authentication (MFA)

Needed capacities or functions

- MFA should be enabled on remote access to the internal network and across all systems and applications in which it is available, such as case management system ("CMS"), document management system ("DMS"), phone system, and finance/accounting software.

Important Considerations and Best Practices

MFA is a security system that requires more than one method of authentication to verify a user's identity for logging in. For example, this can apply to Office 365 (Email, SharePoint, OneDrive and Teams) and Remote Access, along with other cloud-based applications. MFA is one of the most effective tools for stopping cyber threat actors who try and log into your accounts.

Organizations should consider looking into an identity-management solution, such as Okta, Google, or Microsoft 365/Azure, to provide protected access to organizational information systems, where feasible.

11.3 Baseline for Security – Cloud Computing and Policies

Needed capacities or functions

- Have policies addressing staff use of program-controlled cloud services and governance around staff use of personal cloud services accounts not controlled by the program. Staff should not be storing case-related or client information in personal accounts.
- Understand terms of use, privacy policy, data ownership, security, and data portability when moving applications or data to the cloud.
- Increase awareness of backup policies by any of its cloud-services' vendors to assess if there are additional backup needs, in which a third-party solution may be needed (e.g., some programs may need files restored that were no longer backed up by the vendor after a certain period). If data is encrypted and you have your own backup, third-party backups may make restoration of data easier in the event of a security incident. The legal team or general counsel should review its cloud-services policies.
- Users with access to company data in the cloud or office should be accessing data from an organization's device, not personal, unless BYOD and MDM are in place. Keeping data on organization devices allows IT to have control over the data.

Important Considerations and Best Practices

If staff need access to third-party applications through personal accounts, programs should consider business accounts managed by the organization.

With any cloud-based provider, programs should be aware of the levels of access that the provider has to your data and the controls in place that could limit access as needed.

11.4 Baseline for Security – Password Management

Needed capacities or functions

- Educate staff on password security and best practices, such as avoiding using the same passwords for multiple accounts, not sharing passwords, and not writing down passwords, to safeguard client and confidential data.
- IT-related credentials should be stored in a reputable, secure password manager system.

Important Considerations and Best Practices

- IT should subscribe to CISA.gov updates and vendor notifications or advisories for the password manager that is used, in order to stay up-to-date on potential security threats or vulnerabilities of its software and/or service.
- IT should consider backing up its password manager or retaining a secure local copy in the event that a cloud-based password manager has an outage or experiences possible technical issues.
- In addition to IT-related credentials, organizations may want to consider storing other credentials for accounts that store sensitive data, such as HR, Finance, etc.

11.5 Baseline for Security – Mobile Equipment for Staff Use

Needed capacities or functions

- Establish policies to govern the use of organization-owned mobile equipment (e.g., laptops, phones, tablets, etc.) to ensure security, data integrity, and data storage.
- If applicable, organizations should establish policies to govern when employees can bring their own devices ("BYOD") and what they can do with them. Policies should address who may access what services, level of support, remote wipe of organization data, cloud-based backups, and termination/revocation.

Important Considerations and Best Practices

Providing mobile access to work systems and information is inevitable in a modern law office. Fortunately, effective use of mobile equipment provides greater work flexibility and can boost firm productivity.

Regardless of whether a program adopts a BYOD policy or furnishes staff with program-owned mobile devices, a mobile use policy is necessary to protect important information systems and data. Mobile policies should, at least, ensure that:

- Devices are protected with at least a four-digit numerical PIN, if not a more complex password;
- An administrator can remotely wipe organization data on any mobile device used for work purposes;
- System access and work data stored on the device can both be easily removed when an employee leaves the program.

Organizations that have implemented a Bring-Your-Own-Device ("BYOD") policy should take into consideration increased support and security-related costs that come with managing a more diverse range of devices and operating systems.

11.6 Baseline for Security – Mobile Device Management (MDM)

Needed capacities or functions

- Have a solution in place to manage data stored on personal devices and remotely wipe organization data in the event of loss or theft. IT can utilize cloud-based endpoint management solutions that are currently available to them, such as Intune or Google Workspace MDM.
- Provide security of tablets, mobile devices, flash drives, and laptops including remote wipe and/or encryption.

Important Considerations and Best Practices

- Endpoint management solutions are necessary for safeguarding organization and client data that are stored on company-owned and personal devices.
- In addition to endpoint management, IT may consider more advanced options for extra security in the event of a lost or stolen device, such as Geo-tracking or Geo-fencing.

11.7 Baseline for Security – Security Awareness Training

Needed capacities or functions

- Provide cybersecurity training with all staff at least annually.
- Implement a security awareness training platform to conduct phishing tests, identify risk users, and improve the overall security and risk posture of the organization.

Important Considerations and Best Practices

- Research suggests that human error is involved in more than 90% of security breaches.
- Educating users on security awareness improves your organization's first line of security protection.
- Cybersecurity training helps the organization from cyber threats by training staff to identify potential risks before inadvertently exposing the organization and its client data.
- Cybersecurity experts recommend staff receive Cybersecurity Awareness Training at least once every six months to stay up-to-date on the latest threats and best practices.
- In addition to staying up-to-date on the latest threats, shorter, more frequent cybersecurity training combats "training decay" and improves retention of information

11.8 Baseline for Security – Disaster Recovery Plan

Needed capacities or functions

- Have a Disaster Recovery Plan ("DRP") that outlines mission critical procedures, roles, and responsibilities of key staff during a significant system loss or emergency (e.g., data loss, natural disasters, power outages, server failure, ransomware, etc.) to ensure that the organization can

continue its essential operations after a disruptive event. This plan should be reviewed annually and periodically tested.

Important Considerations and Best Practices

- Disaster recovery planning is critical for preparing an organization in the event of an unexpected emergency or disruption, minimizing periods of downtime that can negatively impact clients, and helping recover systems and data in a timely and efficient manner.
- Having a DRP can also help organizations comply with regulatory requirements, such as data protection laws and business continuity standards.
- A well-designed DRP would include procedures for returning to normal services once the emergency has ended.

11.9 Baseline for Security – Incident Response Plan

Needed capacities or functions

- Have an Incident Response Plan that defines an immediate response plan once an organization becomes aware of a security incident, the roles and responsibilities, reporting requirements, communication strategies, etc.
- Incident Response Testing should take place at least once every year with simulated incidents to ensure that the plan remains effective.

Important Considerations and Best Practices

- Incident response planning is primarily focused on the detection, containment, and recovery of a specific security incident or breach, while disaster recovery planning is a broader plan that covers the whole business enterprise during a range of disruptive events.
- One of the key benefits of incident response planning is that it can improve an organization's ability to quickly and accurately identify security breaches. The plan typically includes procedures for detecting and analyzing different types of security incidents as well as the systems and data that may have been compromised.

11.10 Baseline for Security – Endpoint Detection and Response (EDR)

Needed capacities or functions

- Deploy EDR technologies, which are the latest tools to combat risk of viruses, such as malware, spyware, and ransomware. They provide proactive means to identify and mitigate risks by isolating endpoints from the network and, thus, spreading further than the single point of attack.

Important Considerations and Best Practices

- While most organizations only use anti-virus ("AV") solutions, AV is becoming less effective at detecting and preventing evolving malware and the methods used by cyber threat actors that are becoming increasingly sophisticated. EDR is critical for enhancing an organization's endpoint security posture. More organizations are now adopting EDR as a supplement to their existing AV solutions or as part of a broader endpoint security platform. EDR technologies provide a more

advanced level of protection against new and emerging threats that may evade traditional AV and use behavioral analysis and machine learning to proactively address potential threats
- Programs should consider EDR technologies for all servers and endpoints. Examples of EDR technologies include Windows Defender, Sentinel One, and Sophos XDR.

11.11 Baseline for Security – Email Security

Needed capacities or functions

- Implement email security filtering tools that provide protection against emails containing malware, malicious links and attachments, phishing, etc.

Important Considerations and Best Practices

More advanced or enhanced built-in security may require additional licensing. Built-in email security / filtering tools (e.g., Office 365 or Google) may not provide enough protection. For any email security / filtering system, IT should assess if it is working effectively. Programs may need to consider third-party tools, such as Mimecast, Proofpoint, etc.

11.12 Baseline for Security – Cyber Insurance

Needed capacities or functions

- Investigate and strongly consider purchasing cyber insurance from a reputable insurance broker.
- Discuss with your legal counsel whether your firm's current coverage is sufficient considering the types of information you are storing, your current security practices, your malpractice coverage, etc.

Important Considerations and Best Practices

Cyber insurance is essential in helping your organization recover after a data breach. Insurance can help with costs that can include business disruption, equipment damage, legal fees, public relations expenses, forensic analysis, and costs associated with legally mandated notifications. Insurance also helps companies comply with state regulations that require a business to notify customers of a data breach involving personally identifiable information.

Programs should have cybersecurity insurance in place in the event of a cybersecurity breach. Programs should be aware of their legal and ethical duties, including reporting to the clients and relevant legal authorities, in case of a breach.

12 Training

12.1 Baseline for Training – Training and Technology

Needed capacities or functions

- Conduct regular technology staff surveys to identify training needs and priorities organization-wide.

- Provide adequate internal capacity or outsourced support for onboarding and ongoing technology-related trainings.
- Provide training and support for all personnel in the use of appropriate systems, software, and security best practices. As organizations develop new tools for clients, staff should be adequately trained to provide support on these tools.
- Train IT on existing policies for technology use and ABA ethical standards on technology.
- Use of technology to deliver training, including, where appropriate, webinars, online meetings, web chat and web conferencing tools, and hands on/in person training.
- Set technology standards for new hires and incorporate technology training as part of an employee orientation process.

Important Considerations and Best Practices

- Trainings are essential for staff to learn the skills and technologies to be effective at their work and, as a result, improve the delivery of client services. However, it is common that trainings are limited or underinvested.
- Trainings can reinforce organizational case management or document management protocols, such as file naming or storing locations, in which staff will need to be regularly refreshed on.
- An organization should consider best practices for effective trainings and training documentation, such as the following:
    - Trainings that are user-focused, based on roles and common tasks that staff need to manage to accomplish their work.
    - Recordings and developed resources stored in a shared, widely known location or centralized knowledge bank for staff to easily access.
    - Keeping trainings short (e.g., 20 minutes) and addressing specific needs to avoid overloading staff.
- Consider leveraging existing resources for written training materials and online learning available (e.g., Microsoft 365 documentation) as needed. These materials can be curated and made appropriate for a given role and task.
- Integrate IT policies into onboarding or technology training to help ensure users not only learn how to use the systems and services but also understand potential dangers and responsibilities such use entails. This is particularly true regarding remote and mobile device access to organizational data and systems.
- Grantees are encouraged to take advantage of national training venues for legal services and non-profits.

12.2 Baseline for Training – Use of technology to deliver training on substantive law, legal skills, and administrative policies and procedures

Needed capacities or functions

- Technologically supported skills, substantive, and administrative training, such as access to on demand training packages, including webinars and other online trainings and podcasts.

Important Considerations and Best Practices

- Participate in educational webinars that LSNTAP provides each year.

- Invest in staff members to attend LSC's annual Innovations in Technology ("ITC") conference.
- Consider the implementation of an online training platform or learning management system that can enable the creation of custom curricula of skills and knowledge for various job roles. Staff can be assigned a learning curriculum and quizzed on the skills and knowledge and additional learning modules can be added as new technologies or skills are needed for the job.

13 Communication and Collaboration

13.1 Baseline for Communication and Collaboration – Email, email lists, and standard collaboration tools

Needed capacities or functions

- Streamline applications in use for collaboration by establishing standard collaboration tools organization-wide and developing clear internal policies for proper use of email and other electronic communication tools.
- Reduce heavy reliance on emails for internal collaboration, which usually involves emails being sent between staff that have attachments with track changes or non-editable versions when real-time collaboration is needed.
- Use email lists by substance and administrative function, as appropriate.
- Develop and use collaborative work environment tools such as blogs, wikis, cloud-based collaboration tools (e.g., Microsoft Teams), and web conferencing for internal and external communication.
- Where applicable, encourage staff to use document links, instead of downloading and emailing documents. This will help ensure that everyone is working on the same version of the document and help improve efficiency.

Important Considerations and Best Practices

- Consider leveraging collaboration tools that are available within the suite of tools of your operating system and streamlining their use.
- Increased use of technologies, such as Wikis, blogs, instant messaging and collaborative work spaces as well as email give rise to issues regarding privacy expectations. The program should have clear policies that govern appropriate use of such technologies and notify employees and others of the degree to which the information shared in them is private.
- Because of the proliferation of overlapping collaboration and communication features across multiple systems, ensure that your organization has clear guidance on which communications and collaboration tools will be used for which purposes. For example, if you have both Microsoft Teams and a VOIP system that allows for instant messaging, determine which of the two systems should be used for internal team chats.

14 Administration

14.1 Baseline for Administration – Internal communication mechanisms

Needed capacities or functions

- Use of an internal communication mechanism/s for communications to staff (e.g., email, email lists, blogs, web conferencing).
- Have a ticketing system or helpdesk software for tracking and monitoring user support tickets and technology issues.
- Determine how to handle after-hours support and communicate expectations with staff (e.g., issues reported after hours will be addressed the next day, no after-hours support but emergency contacts are provided, etc.)

Important Considerations and Best Practices

- Technology can help facilitate internal program communications and depending on the setup of an organization a variety of tools could be considered, including an intranet using tools such as a Google site, SharePoint site or WordPress site. Email lists, SMS, web conferencing and video conferencing tools can also help enhance and facilitate internal communications.
- Ticketing systems help organizations better prioritize, manage, understand their support needs as well as identify broader or systemic problems early. Organizations may also want to consider ticketing systems for other operational functions, such as finance and human resources.
- There are several free or relatively low-cost ticketing system tools and helpdesk software. However, an organization should do a full evaluation of its needs to determine which tool/software best fits its needs.

14.2 Baseline for Administration – Human Resources Information System (HRIS)

Needed capacities or functions

A Human Resources Information System ("HRIS") should be cloud-based and have the capacity to manage these functions:

- Maintain all appropriate personnel records electronically, including:
    - Payroll;
    - Timekeeping;
    - Benefits administration;
    - Maintain confidentiality of personnel data;
    - Advertise positions, track, and accept applications electronically.
- Generate appropriate and necessary personnel reports.
- Enable paperless workflows and processes such as employee onboarding, open enrollment and payroll processing.
- Ability to require multi-factor authentication ("MFA") for administrators and users to gain access to the system or use related technologies, such as single sign-on ("SSO") identity management.

Important Considerations and Best Practices

- An HRIS serves as the hub where employees and managers can access up to date information relevant to the workforce. The automation streamlines all people systems and reduces the risk of errors by reducing manual work.
- Personnel, procedural and administrative manuals can be made available and constantly updated on an intranet site, centralized knowledge base, etc.
- The ease with which staff members can obtain information such as available health benefits or remaining vacation days of sick leave can impact on their receptivity to other forms of technology.

14.3 Baseline for Administration – Accounting

Needed capacities or functions

Accounting systems should be cloud-based and have the capacity to manage these functions:

- Chart of accounts that adequately meets reporting and management needs;
- General ledger, payables, receivables and fixed assets;
- Allocate Payroll;
- Properly allocating costs across funding sources and cost centers;
- Maintain client trust accounts;
- Segregation of funds within the accounting system by GL account;
- Tracking and accounting by funding source (e.g., receipts, expenditures, obligations);
- Tracking and accounting for capitalized assets (e.g., cost, accumulated depreciation, funding source(s), gains/losses from disposal;
- Collecting and reporting financial data for planning, controlling, budgeting, measuring, and evaluating direct and indirect costs;
- Fully describe transactions that flow to the GL through subsidiary journals;
- Financial reporting that is accurate, current, complete, and compliant with financial reporting requirements;
- Ability to require multi-factor authentication (“MFA”) for administrators and users to gain access to the system or use related technologies, such as single sign on (“SSO”) identity management;
- User-specific access privileges;
- Open architecture to integrate with other systems and data sources, such as payroll and bank feeds; and
- Automated accounts payable and credit card applications are necessary.

Important Considerations and Best Practices

- Organizations may consider allocation and revenue recognition modules, dashboard functionalities, and donor database integrations.
- To the extent that such opportunities exist, program management should seek to have its administrative personnel attend pertinent technology training and become involved in support networks that address the use of technology in program administration.

14.4 Baseline for Administration – Grants Management

Needed capacities or functions

Grants maintenance system that can perform the following functions:

- Ability to integrate with the case management system ("CMS") for easier tracking of cases and activities relating to specific grants
- Track information on grant applications and proposals
- Track information on grant requirements, restrictions, and commitments;
- Track payments, remaining balances, and activities throughout the grant term
- Manage reimbursables;
- Calculate indirect costs;
- Track changes or amendments to grants
- Provide control of expenditures against budget;
- Generate reports and track deadlines; and
- Manage contact information.

15 Development and Fundraising

15.1 Baseline for Development and Fundraising – Fundraising and marketing

Needed capacities or functions

- In addition to general legal information available on a statewide website, the organization itself should have a compelling web presence that includes:
    - Description of what services the program offers;
    - Information about volunteer and donation opportunities, as appropriate;
    - Ability to donate online; and
    - Use of a modern content management system to enable staff to quickly and easily update it.
- Should an organization use social media, it should have a strategy on how to use social media to reach out to different target audiences, such as potential supporters, volunteers, and donors.
- Electronically track the contact information, donation and contact history for each individual donor, if the organization has individual donors.
- Ability to generate reliable reports of donors that meet specific criteria, such as interests and giving history.
- Generation of letters, reports, and other appropriate documents.

Important Considerations and Best Practices

- Consider using a Customer Relationship Management ("CRM") system to track donor contacts and history. CRMs like Salesforce, CiviCRM, Raiser's Edge and DonorPerfect are developed specifically for non-profit fundraising, and many also have features to manage volunteer contacts and activities.
- For CRM applications, critical requirements would include:

  - Contact and account management;
  - Partner relationship management (“PRM”);
  - Opportunity and pipeline management;
  - Customer Contract Management;
  - Customer support portal;
  - Reporting, dashboards and forecasting;
  - Integration APIs.
- If using a CRM, it should integrate with the accounting system and become a subsidiary ledger so that all grants, donors, and money received go to CRM, then flow to the accounting system.