Administrative Policies

The Standards for Excellence® Institute
1500 Union Avenue Suite 2500
Baltimore, MD 21211
Phone: 410-727-1726
www.standardsforexcellence.org
PREAMBLE
America’s nonprofit sector serves the public interest and plays an essential role in our society and economy. Hard at work strengthening communities across the nation, nonprofits enrich our lives in a variety of ways by creating a broad array of benefits to society in fields such as charitable, religious, scientific, economic, health, cultural, civil rights, environment, and education.

Public investment and confidence drive the success of nonprofit organizations. Individuals, corporations, foundations, and federal, state, and local governments add value to the services that nonprofits provide by investing time, resources, and funds.

The Standards for Excellence Institute aims to raise the level of accountability, transparency, and effectiveness of all nonprofit organizations to foster excellence and inspire trust. The Standards for Excellence code (Standards, or code) provides a framework and step-by-step guidelines to achieve a well-managed and responsibly governed organization.

The code builds upon the legal foundations of nonprofit management, governance, and operations to embrace fundamental values such as honesty, integrity, fairness, respect, trust, compassion, responsibility, and transparency. The code consists of six Guiding Principles in 27 topic areas with specific performance benchmarks that characterize effective, ethical, and accountable organizations. The Institute helps the nonprofit sector operate in accordance with the Standards for Excellence code by providing educational resources, assistance, and a voluntary accreditation process.

The Standards for Excellence Institute encourages all nonprofit organizations to adopt the Guiding Principles of the Standards for Excellence code. By implementing the performance benchmarks in the code, nonprofit organizations will meet the highest ethical standards for effective service in the public interest.

STANDARDS FOR EXCELLENCE - GUIDING PRINCIPLES

I. MISSION, STRATEGY and EVALUATION
Guiding Principle: Nonprofits are founded for the public good and operate to accomplish a stated purpose through specific program activities. A nonprofit should have a well-defined mission, and its programs should effectively and efficiently work toward achieving that mission. Nonprofits have an obligation to ensure program effectiveness and to devote the resources of the organization to achieving its stated purpose.

II. LEADERSHIP: BOARD, STAFF, and VOLUNTEERS
Guiding Principle: Nonprofits depend upon effective leadership to successfully enact their missions and programs. Effective leadership consists of a partnership between the board and management, each of which plays an essential role. Understanding and negotiating these shared and complex elements of leadership is essential to the organization’s success. A nonprofit’s employees and volunteers are fundamental to its ability to achieve its mission.

Board members are in a position of trust to ensure that resources are used to carry out the mission of the organization. An organization’s board leadership should consist of volunteers who are committed to the mission and who demonstrate an understanding of the community served. An effective nonprofit board should determine the mission of the organization, establish management policies and procedures, assure that adequate human and financial resources are available, and actively monitor the organization’s allocation of resources to effectively and efficiently fulfill its mission.

Nonprofits should also have executive leadership which carries out the day-to-day operations of the organization, ensures financial and organizational sustainability, and provides adequate information to the board of directors. An organization’s human resource policies should address both paid employees and volunteers and should be fair, establish clear expectations, and provide meaningful and effective performance evaluation.

III. LEGAL COMPLIANCE and ETHICS
Guiding Principle: Nonprofits enjoy the public’s trust, and therefore must comply with a diverse array of legal and regulatory requirements. Organizations should conduct periodic reviews to address regulatory and fiduciary
concerns. One of a leadership’s fundamental responsibilities is to ensure that the organization governs and operates in an ethical and legal manner. Fostering exemplary conduct is one of the most effective means of developing internal and external trust as well as preventing misconduct. Moreover, to honor the trust that the public has given them, nonprofits have an obligation to go beyond legal requirements and embrace the highest ethical practices. Nonprofit board, staff, and volunteers must act in the best interest of the organization, rather than in furtherance of personal interests or the interests of third parties. A nonprofit should have policies in place, and should routinely and systematically implement those policies, to prevent actual, potential, or perceived conflicts of interest. Ethics and compliance reinforce each other.

IV. FINANCE AND OPERATIONS
Guiding Principle: Nonprofits should have sound financial and operational systems in place and should ensure that accurate records are kept. The organization's financial and nonfinancial resources must be used in furtherance of tax-exempt purposes. Organizations should conduct periodic reviews to address accuracy and transparency of financial and operational reporting, and safeguards to protect the integrity of the reporting systems.

V. RESOURCE DEVELOPMENT
Guiding Principle: The responsibility for resource development is shared by the board and staff. Nonprofit organizations depend on an array of sources of financial support. An organization's resource development program should be maintained on a foundation of truthfulness and responsible stewardship. Its resource development policies should be consistent with its mission, compatible with its organizational capacity, and respectful of the interests of donors, prospective donors, and others providing resources to the organization.

VI. PUBLIC AWARENESS, ENGAGEMENT, and ADVOCACY
Guiding Principle: Nonprofits should represent the interests of the people they serve through public education and public policy advocacy, as well as by encouraging board members, staff, volunteers, and stakeholders to participate in the public affairs of the community. When appropriate to advance the organization’s mission, nonprofits should engage in promoting public participation in community affairs and elections. As such, they should communicate in an effective manner to educate, inform, and engage the public.

ABOUT THE STANDARDS FOR EXCELLENCE INSTITUTE
The Standards for Excellence Institute is a national initiative established to promote the highest standards of ethics and accountability in nonprofit governance, management, and operations, and to facilitate adherence to those standards by all nonprofit organizations. The Institute uses as a vehicle the Standards for Excellence program, a system of nonprofit sector industry self-regulation originated by the Maryland Association of Nonprofit Organizations and currently replicated by licensed partners in Alabama, Delaware, the District of Columbia, Ohio, Oklahoma, Memphis, Pennsylvania, and Virginia. The program is also being offered to chapters of The Arc nationwide through The Arc of the United States, to the American Nurses Association, to the Sacred Sector program of the Center for Public Justice, to Catholic nonprofit organizations nationwide through the National Leadership Roundtable on Church Management, and through the Markkula Center for Applied Ethics at the Santa Clara University.

The centerpiece of the Institute’s program is the Standards for Excellence: An Ethics and Accountability Code for the Nonprofit Sector. The Institute also makes available to member organizations a comprehensive system of educational tools to enable individual nonprofit organizations to improve their governance and management practices. Standards for Excellence accreditation is available to individual organizations through a rigorous peer review process in selected locations and nationwide through The Standards for Excellence Institute.

For more information about joining The Standards for Excellence Institute or to obtain additional copies of the booklet or educational resource packets visit our website at www.standardsforexcellence.org.
ADMINISTRATIVE POLICIES

As the Standards for Excellence: An Ethics and Accountability Code for the Nonprofit Sector states:

A nonprofit should have written board-approved administrative policies that are periodically reviewed by the board. At a minimum, these policies should address issues such as crisis and disaster planning, information technology, communications, and social media.

Every nonprofit organization continuously encounters various scenarios, and issues, that require management, staff, and volunteers to act in accordance to the organization’s expectations beyond those outlined in the charter, bylaws, and other essential documents. These expectations – or guidelines – should be formulated by each individual organization and approved by the board of directors as administrative policies. The scenarios and issues faced by each group vary significantly. While some issues may be short-term and simpler to address, others could result in great losses to the organization and may even involve interruption in operations. Well-articulated administrative policies help organizations carefully handle important administrative functions so that they are in the best position to fulfill their important missions.

This educational resource packet focuses on the importance of developing and abiding by strong administrative policies as they pertain to crisis and disaster planning, information technology, communications, and social media, and it provides guidelines to consider when formulating these administrative policies.

Crisis and Disaster Planning

The very nature of crises and disasters is that they are unplanned, unexpected, and have serious impact on people, organizations, and communities. In the United States, recent examples include the 9/11 terrorist attacks, Hurricane Katrina, Superstorm Sandy, category 5 tornados, and other natural disasters. Around the world, we see armed struggles, terrorism, and other man-made and natural events and the upheaval they produce.

These events capture the nation’s attention, bring community members to action as volunteers and donors, and remind all that emergencies and devastation can come at any time, at any place.

Generally, emergencies can affect five key areas:

- Physical or psychological injury to people
- Inability to continue important organization operations
- Damage to or destruction of facilities
- Financial loss, apart from the above
- Spillover effects from something that has affected some other person or organization

Many businesses, corporations, government agencies, and other entities have designed a variety of resources, tools, plans, and actions to guide their response to crises and disasters. You will find several of these examples in the resources and attachment sections of this educational resource packet.
Importance for Nonprofits
Nonprofits occupy a key role in the response to disasters. Nonprofits are often at the forefront of supporting those affected by disasters. Agencies such as international disaster and relief organizations, hospitals, health and human services, food and housing organizations, and animal rescues are part of the first responder teams in many emergencies – and many of these organizations continue to provide support long after the immediate event. Maintaining the nonprofits’ health, strength, and capacity to serve others is vital to their community and constituents.

Nonprofits also hold a unique place in the public trust and often come under intense media scrutiny. Crises such as financial or ethical impropriety on the part of any member of the organization can seriously damage its reputation or ability to continue providing services. Even irresponsible actions by others in your field or in the larger nonprofit sector can have a negative spillover impact on your organization. A proactive approach to addressing these issues will help you come out on top after a crisis.

Safeguarding the knowledge, skills, relationships, passion, and creativity of its human resources is an essential component for every organization. In the nonprofit sector, the contribution of the board and staff are even more critical. Many nonprofits operate with a small group of leaders, often playing multiple roles. The unexpected loss of any member of organizational leadership presents a challenge for nonprofits, and the potential loss of several key leaders in a disaster situation can produce a major crisis for many nonprofits.

Dealing with Crisis
Crisis management is defined as “an organization’s pre-established activities and guidelines for preparing and responding to significant catastrophic events or incidents . . . in a safe and effective manner.”

The Crisis and Disaster Plan is a key tool that documents the actions the organization will take in the event of a significant event, crisis, or disaster.

Benefits of a Crisis and Disaster Plan
The focus on crisis and disaster planning ensures that a nonprofit can:
- Prepare for emergencies, to the extent possible
- Respond quickly and clearly to all constituents
- Continue to offer its essential programs
- Resume full operations, as soon as possible
- Safeguard and protect vital organizational resources

---

Risks of Not Addressing the Issue
Without a Crisis and Disaster Plan, during and after a crisis, a nonprofit may not be able to:

- Provide essential services
- Generate earned and philanthropic revenue
- Retain or replace key organization leaders
- Avoid negative media attention
- Safeguard its intellectual property
- Maintain public confidence

Components of a Crisis and Disaster Plan
The components are introduced briefly below and samples are provided in the attachments section of this educational resource packet. Depending on the type of services your organization provides and the environment in which you work, you may find that the components of your crisis and disaster plan may need to be more highly developed in some areas than others. You may also find that your organization requires additional components to adequately prepare for disasters.

It may also be helpful to reach out to other similar organizations working in your field or region to explore and compare disaster and crisis planning approaches.

A. Define the Purpose, Priorities, and Principles
Start your plan with an explanation of why and how the crisis and disaster plan is relevant to your organization, its mission, and the people you serve. This communicates the organizational commitment to addressing crisis situations in a focused and efficient way that safeguards the mission and assets held in the public trust. (See Attachment A “Sample Plan Introduction.”)

B. Designate the Response Team
The response team provides the structure, establishes the principles, and implements the policies for action in the event of an emergency. The plan describes roles and responsibilities of team members and provides up-to-date contact information for the individuals involved. (See Attachment B “Sample Roles and Responsibilities of the Disaster/Crisis Response Team.”)

C. Assess Your Risk through Different Types of Crises and Disasters
Events may occur that are either external or internal to the organization and both will have serious impact on your capacity. Take into consideration your location, community, and program focus in defining and prioritizing the risks that are most relevant to you. (See Attachment C “Sample Risk Assessment Worksheet.”)

D. Develop the Business Continuity Plan
Business continuity planning addresses the following areas:

- **Preparation** – actions taken prior to a crisis or disaster
- **Response** – procedures and steps done immediately after an emergency or interruption to business
- **Recovery/Restoration** – steps taken to restore functionality so that some level of mission driven service can be offered to clients while restoring the organization to its original status
The Business Continuity Plan is an important tool and its development will depend upon many factors, including, but not limited to the mission of the organization, the services provided, and the communities served. (See Attachment D “Sample Continuity Plan Worksheet.”)

Additional Considerations

Other Policies, Procedures, and Plans: As you develop your plan, it is likely that you will begin to see the connections between crisis and disaster planning and the policies, procedures, and operational plans that your organization has in place during non-disaster times. In some cases, a strong and well planned systematic response can lessen the impact of a crisis or disaster. An established and well-functioning system of crisis and disaster response can make for a quicker response and ease tensions and anxieties about an unexpected event. The development of your crisis and disaster plan should include a review of all related systems, plans, and procedures including:

- Board, staff, and volunteer policies
- Program/service standards and compliance
- Insurance and risk management policies
- Technology recovery and cyber-security policies
- Communications/social media policies
- Financial policies, including internal controls, purchasing, reserves, policies on uncovering improprieties
- Succession planning and leadership development plans
- Resource development plan

Supporting Those You Serve: Nonprofit organizations providing direct services to individuals, families, and communities have a special and heightened interest, need, and obligation to ensure that those who rely on their services continue to receive needed services and assistance. Many nonprofits offer essential direct services on an ongoing and regular basis (health and mental health, food, nutrition, public safety, to name a few.) Procedures should address how the organization will address safety, basic operational needs, and ensure accurate and timely information and instructions for those individuals and communities the nonprofit serves.

Supporting Other Stakeholders: Nonprofits may also want to consider their role in providing important disaster-preparedness information and resources to their stakeholders. The American Red Cross (http://www.redcross.org/prepare) and the federal government website, Ready.gov, both have a wide range of materials covering many types of disasters, checklists, and tools for families, schools, and workplaces. Providing your stakeholders with access to these resources on a regular basis will help them and their families be better prepared in cases of emergencies.

Special Events: Crises and disasters can also have an impact on a single event sponsored by a nonprofit, such as a fundraiser, conference, or meeting. Obtaining cancellation insurance may provide a financial cushion for this type of occurrence.
Volunteers: In a disaster or crisis, volunteers can play a major role in both the response and recovery phases. Volunteers might temporarily fill in for staff members who are unable to work, free up staff to focus on critical services, and/or provide aid and support to clients and community members. You can make the best use of this valuable resource by planning and identifying the ways you will recruit, train, and manage volunteers during a crisis.

Crisis Communication
Implementing a crisis communications plan is an essential part of a nonprofit’s crisis and disaster preparedness efforts. In the event of a crisis, a nonprofit must be able to communicate with all stakeholders with confidence, speed, and accuracy. Protecting the positive public image of your organization and ensuring the public confidence are the main goals of your crisis communications plan.

When a disaster or crisis arises, your organization should have a well-considered plan of action to communicate both internally and externally to all stakeholders including the public and media. This plan identifies who will (and will not) speak on behalf of the organization, how the messages will be developed, how all staff and board members will be prepared to deal with inquiries, and how the response will be evaluated afterwards so that improvements can be made to the plan, as needed.

Begin by brainstorming about the types of crises, disasters, or emergencies that might arise, no matter how unlikely – think about situations that are typical for your type of organization given your location, community, and program focus. Once you have a list of potential disasters and crisis, prioritize those that are most relevant.

Here are a few scenarios to consider:
- Damage to facilities that seriously affects your ability to operate
- Natural disaster that prevents clients, staff, or volunteers from being able to access your facility
- Workplace violence involving a client, staff, volunteer, or board member
- Death or serious illness involving a staff or board member that seriously affects your ability to operate
- Criminal activity involving a client, staff, volunteer, or board member
- Improper conduct involving a client, staff, volunteer, or board member
- Widespread staff or board resignations
- Fraud or major theft
- Unfavorable action by a funder, auditor, or regulatory body
- Suspension or loss of license
- Outside event that involves your organization’s areas of expertise where you may be asked to comment or take a position (for example a situation involving mental illness, immigration, child or spouse abuse)
- Proprietary information, rumors, or falsehoods spread through social media

Steps in Developing a Crisis Communication Plan
- Define key stakeholders/priority audiences
Think broadly when identifying stakeholders – consider employees, volunteers, board members, those with whom you do business and those you serve, and other organizations and people with a stake in your organization.

- **Organize all relevant contact information**
  This includes information about staff, volunteers, board, clients, partners, funders, vendors, media, and local emergency services. Make sure this information is kept current. Access to the information should be available and accessible to several people in different locations, if an emergency prevents access to your facility or computer systems.

- **Develop your message and disseminate**
  In a crisis or disaster, a clear, timely, and thorough response is essential. This allows your organization to frame the issue, present the facts, and demonstrate to the public that you are taking positive action. This is also an opportunity for you to engage the public’s support as you recover from the crisis.

- **Evaluate your response and revise your plan**
  After the crisis is over, take a critical look at your crisis communication – what worked, what could be improved, what else was needed, and so on. Incorporate your findings into plan revision and staff training.

*(See Attachment E “Sample Emergency/Crisis Communication Plan.”)*

**Information Technology**

Information Technology (IT) is one of the few areas in organizational policy that regularly touches on almost every aspect of the organization. It is rare for any of us to go through the day without interacting with something that is plugged into the wall, charged overnight, or relies on data that we have collected. We talk on phones, type letters, e-mail, log data, research online, give presentations, use key fobs to access buildings – often without even realizing the infrastructure needed to support these common practices. Beyond just the physical technology, there is also the data, the networks, and well-developed virtual realities (websites and social media) that contain critical (as well as confidential and private) information.

Imagine what happens when the power goes out at your facility. Your staff may physically be able to deliver your services, but your “back-office,” the whole set of systems and resources that support program delivery, is ground to a halt. Adequate supportive IT policies ensure that the people within an organization understand the role that technology and data play in the organization. It raises awareness of the demands technology needs place on the organization and what efforts need to be taken to keep the critical infrastructure secure, reliable, and sustainable.

While it is truly mission-critical, many organizations treat IT policy and planning as either secondary to program development or only in response to either major or minor disasters, where processes are not evaluated until something goes very wrong. For IT to be effective, it must grow in tandem with the rest of the organization. Thinking of IT holistically, as an important part of the greater whole secured through board approved policy, will ensure that it is being utilized to its fullest potential and serving the broader goal of facilitating mission delivery. When IT is used properly, it is a significant value-generator. When IT is used improperly, it can become the Achilles’ heel of an organization.
Information Technology (IT)

Information Technology refers to anything related to computing technology, such as networking, hardware, software, data, the Internet, or the people that work with these technologies. Given the “digitization” of more and more things, IT now encompasses most modes of communication as well as things that we normally consider to be computer-related.

Benefits of IT Policy and Planning Include:

- Understanding the current state of technology infrastructure in your organization and whether it is at risk of obsolescence, break down, or under-utilization
- Relating the use of technology to the overall mission and goals of your organization
- Identifying areas where technology can enhance productivity and mission delivery
- Protecting the organization’s systems from failures that can hobble the organization’s ability to work, and identifying root causes of existing technology challenge
- Assessing training and staffing needs to maximize utility of existing systems
- Creating effective fundraising strategies using new technologies

Full Scope of Information Technology

The concept of Information Technology is broad and is growing every day. What used to solely include computers and software is now a vast collection of physical devices, electronic networks, and stored data that interact in increasingly complicated ways. When considering the IT of an organization, it is important to consider all the things that contribute to and come into play when thinking about an organization’s technology infrastructure and demands. Items to keep in mind include:

- New technology developments (social media, cloud computing, etc.)
- Data utilization and demands within an organization
- Acquisition, maintenance, and disposal of physical hardware
- Installation, compatibility, maintenance, upgrade, and licensing of software
- Connectivity of devices to internal and external networks
- Physical and electronic security of equipment and data
- Privacy and information management regulations
- User training
- Staffing requirements
- Responsible use policies for equipment and data
- Social Media’s impact on work, messaging, and reputation

These items, and there are even more, have real costs and impacts on your organization’s ability to meet its mission. In approaching IT, it is important to pay close attention to the real costs (time, upfront investment, ongoing expenses, etc.) associated with it, the benefits to your organization’s ability to fulfill its mission, and the complexity of connections between systems. Rarely, in today’s “connected” world, does any one element of an organization’s technology work in isolation from others.
**Hardware**

The physical devices that constitute our technology environment including: computers, copiers, phones, printers, personal digital assistants (PDAs), smartphones, servers, routers, cables, switches, monitors, cameras, etc.

**Software**

Generally considered the applications that “run” on the hardware and make the hardware perform. Software includes operating systems, databases, web browsers, office productivity suites, Virtual Private Network (VPN) clients, games, etc.

**IT Solutions**

A combination of hardware, software, connectivity, and administrative resources dedicated to supporting operations and program delivery. For example, a website is a solution that requires a computer server with special software, access to the internet, individual web pages written in special programming code, a webmaster, perhaps a database, and a computer with a browser to work.

**IT Policies**

IT policies define and outline the relationship of ongoing interaction between technology and the people that comprise your organization. A single flip of a switch or a few keystrokes can destroy data, prevent access, undo customization, unleash a virus, make private information public, breach confidentiality, overload a system, or shut down machines. Organizations must take deliberate steps to implement policies and procedures that mitigate the risk that can range from system failure to malicious intent. *(See Attachment F “Sample Technology Policy (and Privacy Policy for Users)”).*

**Recommended Components of Information Technology Policies**

A. Acceptable Use
B. Contracting/Outsourcing
C. Data Integrity: Security, Protection, and Backup
D. Monitoring and Usage

*(See attachments for more information and examples of each, as well as a comprehensive sample IT policy.)*

**Acceptable Use**

An acceptable use policy is critical to any set of IT policies. It identifies how data and technology can be accessed, what it can be used for, and how it needs to be handled. These policies and other procedures should clearly identify how information is kept confidential, what can be done on behalf of the organization when using social media, what technology can be used by whom and where, and who has access to what information, just to highlight a few examples.
In considering procedures, be aware that digital information is easily transferable, easily deleted, and easily corrupted. Mechanisms need to be put in place to ensure that the hardware and software are secure and conserve data integrity and that users have appropriate training and access to minimize the potential impact of user error or user malfeasance. *(See Attachment G “Acceptable Use Policies”)*

**Contracting/Outsourcing**

Many aspects of an organization’s IT may be outsourced or contracted. Organizations may have an external company that provides technical support to staff and maintains all or some of the IT infrastructure. Organizations may hire an external contractor to design and maintain the website. Service may be hosted by a third party (cloud computing, server farms, etc.) There are many ways that organizations engage external consultants and contractors to provide pieces of the overall IT management. When outsourcing, organizations should have policies in place that enforce clear agreements and ensure that contractor and third party vendors abide by the organization’s policies. Organizations do not want a vendor to be a weak link in an otherwise robust data integrity system. An IT policy might specify further details regarding outsourced IT services including employee filing of outsourced service tickets. *(See Attachment H “IT Consultants.”)*

**Data Integrity**

Data integrity is a critical component to any IT policy. At the most basic level, loss or corruption of data requires work to be repeated. At its most extreme, trade secrets or private information is stolen and used against the organization or its clients. Ensuring that data are secure, backed up, and handled appropriately is critical and is the responsibility of all staff including the chief executive. Failure to do so can result in lost productivity, violation of regulatory requirements, or fraud. IT Staff need to remain aware of vulnerabilities to data integrity and implement regular and necessary patches and updates to integrity protections.

**Security:** Organizations should have adequate security in place that controls access to data. Generally, this involves controlling who has access to your system through robust login and user rights management. It also includes firewalls that secure internal systems against access from the external networks (this is the internet for most systems.) Security also involves user education as unattended workstations, shared passwords, or lost laptops are the most common access points for security breaches. In instances where remote access to internal systems are allowed, special care must be taken to secure these access methods.

---

<table>
<thead>
<tr>
<th>KEY TERM</th>
<th><strong>Acceptable Use Policy (AUP)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An acceptable use policy is a broad category of guidelines, requirements, and expectations around how users (staff/volunteers/clients) interact with your technology and your data.</td>
</tr>
</tbody>
</table>
Many nonprofits must comply with legal regulations that require compliance with PCI standards\(^2\) (which protect credit and debit cardholder data) or HIPPA standards\(^3\) (which protect individually identifiable health information,) among others. While these standards do require certain technology to be in place, they are largely concerned with the use of these technologies. Your organization should not only secure compliant hardware, but also ensure that your organization is operating in compliance with the standards.

**Protection:** E-mail and web browsing are just two examples of technologies that connect the internal technology systems of an organization with the outside world. Depending on the organization, there may be other avenues including websites, virtual networks, etc. The point is that every system has some point of contact with the outside world and that point of contact is a place for viruses and other malicious elements to enter the system. Organizations should have protections such as virus and malware protection software and other monitoring solutions that mitigate the vulnerability and impact of security breaches. Sometimes forgotten are mobile devices which need to be protected and secured as well.

**Backup:** Simply put, data must be backed up. A simple keystroke can unintentionally delete a file and data can get corrupted for what seems to be no reason at all. Having only one copy is truly a recipe for potential disaster. Organizations should have robust backup solutions in place that ideally backs up information daily and in a manner, that secures information in more than one physical location.

*(See Attachment I “Data Security and Integrity.”)*

---

**Online Fundraising**, the practice of soliciting donations through the Internet via a website or e-mail campaign, requires special attention from IT managers. Your organization will need to consider the following requirements before initiating an online fundraising campaign:

1. **State Registration Rules.** Rules for state registration of nonprofits that engage in online fundraising remain somewhat ambiguous. According to the Charleston Principles,\(^4\) a set of guidelines released by the National Association of State Charity Officials (NASCO), organizations that are physically located in a state and/or specifically solicit online donations in a state should register within that state. Generally, it is not required to register in states in which your organization does not actively solicit donations. However, we recommend that your organization read and comply with the requirements of each state in which you are located and/or solicit donations. For more information, see Standards for Excellence educational resource packet, *Disclose It: A Charitable Nonprofit’s Guide to Disclosure Requirements.*

---


2. **Disclosure Requirements.** Website and e-mail solicitations should comply with the same disclosure requirements as other solicitations. Online solicitations should contain a clear statement of your organization’s name, mission, the intended use of the funds, 501(c)(3) status, as well as disclosure statements required by state law. For more information, see Standards for Excellence educational resource packet, *Disclose It: A Charitable Nonprofit’s Guide to Disclosure Requirements*.

3. **Data Security.** Your organization should establish an official policy to ensure that personal and credit card information received from donors online remains private and secure. While larger nonprofits may choose to build secure online donation platforms in-house, many smaller nonprofits opt to use external donation processing sites like Network for Good, PayPal, or Razoo. Before entering a contract with a third-party site, your organization should consider each service’s processing fees for transactions, donation delivery schedules, collection of demographic information on donors, and capabilities for customization, among other factors.

4. **Additional Regulations.** Online raffles, auctions, and other online fundraising mechanisms may be subject to additional state regulations. Check your state’s specific regulations for detailed information.

---

**Monitoring and Usage**

Monitoring your information technology should not considered spying. Monitoring can indicate what resources are being over or under-utilized and convey important information about the overall health of the systems. Depending on the resource, this can provide critical information for the organization.

Monitoring a website or social media may indicate what messages or online strategies are the most engaging. It may tell you what services people are most interested in and what they want to know about you. Monitoring infrastructure can reveal that you are paying for far more bandwidth than the organization needs to connect to the Internet or that a particular piece of hardware is failing and may need to be replaced.

For staff and other key users, information technology can be a double-edged sword – it can be extremely productive and it can be a big distraction. In addition to acceptable use policies that clearly state what is appropriate use of the organization’s technology, monitoring usage may shed light on who is over and/or under-tasked.

---

Not sure if you should contract out to a consultant or hire more support staff? Check out this article: [http://www.techsoup.org/support/articles-and-how-tos/when-to-use-consultants](http://www.techsoup.org/support/articles-and-how-tos/when-to-use-consultants)

---

**Strategic IT Planning**

The complexity of Information Technologies necessitates the board and staff taking a deliberate look at the systems, data, and staffing required to support fulfilling the mission of the

---

organization. What makes a plan “strategic” is its ability to articulate assumptions and plans for the future and link that to the technology needed to realize that future. Additionally, you need to consider the overall resources, technological and human, needed to bring the plan to fruition.

Strategic IT planning must go beyond a simple tools mindset that would be defined by the “get what you need to get the job done” approach. Technology now can shape how work is done as much as supporting the work itself. Technology can open the doors to totally new models of program delivery. Just consider the development of distance learning, a technology that eliminates the geography and facilities limitations that used to be barriers to education. *(See Attachment J “Getting Started with IT Planning.”)*

<table>
<thead>
<tr>
<th><strong>Key Term</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Needs Assessment</strong></td>
</tr>
</tbody>
</table>

A systematic approach to determining the specific needs of an organization or project. Needs may include accessibility, type of information/data collected or accessed, the infrastructure (hardware/software/connectivity) required, the professional skill set required, or the training needs of users.

Needs assessments are a critical component of any strategic IT planning effort. Planners must have a clear understanding of what the organization is trying to accomplish through mission delivery and then work to identify the technologies and information that will best contribute to efficient and effective work. Often this requires deconstructing the reporting and evaluation process to determine what data are needed, how it will be assessed, and what tools (hardware/software/connectivity) are needed to accomplish the work.

In addition to a needs assessment, organizations should consider conducting an opportunity assessment (assessing whether new technology could allow the organization to provide new services or reach new populations.) For example, creating the technological capacity to build a strong social media presence or design a service-oriented smart phone app could help an organization reach more youth.

Finally, the long-term, strategic element of IT planning must consider the legacy effect of technology. Many technology solutions require substantial investments of time and money. Often organizations are reluctant to assess the limitations of solutions that are already in place because of this investment. Many older IT systems are, in fact, very robust and can meet the needs of an organization if a proper needs and resource assessment is conducted. However, some legacy systems hinder an organization’s move towards greater effectiveness and efficiency in mission delivery. Additionally, the costs of staying with a legacy system may be high as upgrades and service agreements are required to maintain operability. Therefore, strategic IT planning must also include aggressive evaluation of legacy systems to determine their appropriateness to the organization's future work.

**Budget/Ongoing Costs**

Information technology can account for significant expenses for an organization. Hardware and software have limited shelf lives in that they either breakdown, become too slow, or do not have all the tools to meet an organization’s needs. Replacement costs are...
unavoidable. Additionally, maintenance contracts, licensing fees, connectivity charges (phone and broadband,) and hosting fees are typical ongoing costs.

**Total Cost of Ownership (TCO)**
With so many factors contributing to the cost of just a single system, how do we effectively anticipate what our future costs will be? Total Cost of Ownership (TCO) is a calculation of an all-inclusive single value for the complete lifecycle of a capital purchase including upfront acquisition price and more hidden long-term operation costs such as utility costs, operator labor, initial and ongoing training, and maintenance. While the Total Cost of Ownership can vary greatly depending on the capital expense and the organization, supporting new equipment and software can cost between five and eight times the purchase price.⁶

Your organization may need to adjust cost projections if you choose to take advantage of cloud-based technologies. The “cloud” is the provision of computer software and hardware as a service, rather than as a physical product. When considering whether to invest in cloud-based services, your organization should evaluate both the advantages (e.g., reduced start-up costs, access to a variety of services, reduced burden on staff, etc.) and the potential concerns (e.g., data security, possibility that organizations providing cloud-based services may cease to offer the service or go out of business, etc.) associated with the specific service.

Staff time is another expense that is often overlooked when considering IT. Be cognizant of the amount of staff time consumed by managing vendor contracts, performing maintenance (if done in house,) supporting users, training users, navigating cumbersome systems, waiting for things to process, re-entering data, manipulating reports, , etc. When taken in whole, IT administration-related time can add up.

**Communications and Social Media**
Communication is a comprehensive component of any organization’s infrastructure, involving and impacting all aspects of operations and programming. It is in many ways just as important as the effective execution of mission-based initiatives. Promotion, messaging, publicity, engagement, and opinion-shaping influences can determine the ultimate success or failure of those initiatives.

Benefits of establishing communications policies and a communications plan include:
- Increasing public awareness of the organization’s mission and programs
- Widening the organization’s community connectedness
- Ensuring consistency in messaging and public image
- Building synergy and teamwork by involving every component of the organization
- Helping to streamline organizational strategic planning, prioritizing, and actions

---

How to Begin
If there is a member of the board with expertise in communications, they should work with the chief executive to develop a comprehensive communications policy. In the absence of such board expertise, the chief executive should consult with a communications expert or several experts – for example, a human resources expert for internal communications and a social media expert for external communications – and involve key staff in the development of the policy. Once the policy has been approved by the board, the staff should then produce a communications plan to implement that policy under the guidance of executive leadership.

The Communications Policy
An organization’s communications policy should provide clear guidance for each aspect of its internal and external communications. The key elements of a communications policy are:

- **Statement of Purpose** – The policy’s goals may be (1) to ensure consistent projection of the most positive, professional, and accurate organizational image to the public; and (2) to facilitate effective, professional, and respectful communications between and among the board, organizational management, and the staff.

- **Public Relations and Policy Communications/Relations** – Public relations communications are more specific to the organization’s interactions with the media, legislative or other policy-making entities, organizational partners, and entities or individuals with opposing missions. These components of the policy establish specific media contacts within the organization; describe if, how, and in what media the organization may advertise; and may even contain position or briefing papers on specific key topics related to the organization’s mission and values.

- **Internal Communications** – Internal communications policies cover information exchanges among staff, between the staff and the chief executive, between the chief executive and the board, and among the board members. This section of the policy includes e-mail, written, and oral communications; the individuals that are included in certain types of communications; and whether, or the degree to which, personal communications are permitted or restricted in the workplace. Internal communications policies should also include language governing the tone and manner of all modes of communications to foster and sustain a professional work environment.

- **Trademarks, Logos, and Seals** – These are the policies governing the identification of the organization internally and publicly. They include:
  - The specifications (official pantone color number, sizes and proportions, etc.) and permissible placements of the organization logo(s) in both print and electronic media;
• Preferred or required font styles and sizes to be used in all visual communications; and
• References to the organization’s registered trademarks.

An organization’s style guide would also become part of this component of the communications policy. (See Attachment K “Sample Nonprofit Style Guide.”)

• **External Communications** – This is the policy component that governs the organization’s public profile and the projection of its mission and activities to the community and to its constituents. External communications policies provide guidelines on the modes of disseminating program information; guidelines on the use of social media, both organizational and any expectations of staff’s individual use; the approved phrases and key words to be used when describing the organization and its constituents or communities (for example, “people who are homeless” versus “homeless people”; “La Raza” versus “Hispanic” or “Latino/a.”) This policy should also articulate required descriptions, copyright statements, employment policy statements, and legal disclaimers, as well as dictate their required uses in all modes of communication.

• **Privacy, Security, and Confidentiality** – This policy provides guidance on information technology and on the documentation, storage, and dissemination of Personal Identifier Information (PII) such as social security numbers and other personal information about staff and program participants. It also states what contact information can and cannot be released to whom and under what circumstances, and acceptable business use of communications software and hardware resources.

• **Crisis and Disaster Planning** – As mentioned earlier under Crisis and Disaster Planning, the board should develop the organization’s policy for dealing with both “mission-based” and environmental crises and disasters. The policy should identify who is authorized to speak to the media, to staff, and to constituents on behalf of the organization and under what circumstances during a crisis or disaster. It should include any standard responses acceptable for use by other key staff and stakeholders. It should also make provisions for actions, decisions, vital service continuation, and other essential functions in the absence of telephone communications or Internet access in the event of an emergency.

• **Related documents** appearing as attachments to the communications policy may be the organization’s strategic and development plans, other related policies, letterhead and other document samples, and lists of authorized contact persons.

(See Attachment L “Sample Communications Policy.”)

**The Communications Plan**

With the communications policy as its foundation and the organization’s mission as its guide, the organization’s staff should produce a communications plan to articulate and implement the communications policy as approved by the board of directors. The plan often outlines the step-by-step process of managing communications resources toward implementing the organization’s communications policies. The plan should reflect precisely how the roles of board, management, staff, and key stakeholders as articulated in the communications policy will be actualized on a daily, monthly, quarterly, and annual basis, as appropriate.
The key elements in developing a communications plan include:

- **Assignment of Responsibility** – A team of staff and stakeholders should be assembled to spearhead the planning process, with an appointed or elected chair or project leader.

- **Analysis of the Internal Organizational Environment** – This includes (1) a thoughtful review of the organization’s mission and vision statements to establish boundaries; (2) a review of current and future operations status, staff, and material resources; and (3) a review of other active or pending organizational plans (strategic, fundraising, information technology, recruitment, etc.) to ensure that the various parts of the organization are supportive of each other and the mission.

- **Analysis of the Organization’s External Environment** – The team should identify external forces that will impact the organization’s communications content (for example: legislative and/or environmental,) including the organization’s strengths and weaknesses in terms of controlling or shaping that impact.

- **Identifying Service Constituents and Other Target Audiences** – The value and effectiveness of a communications plan centers on its value to the intended recipients. First identify those with whom the organization will communicate and then what those entities and individuals will want to hear and see to ensure the plan’s maximum strategic effectiveness. Members of these recipient groups should be involved in the planning process at this point, as soon as the groups are identified.\(^7\)

- **Messaging** – This includes: what will the organization say, how will it say it, and what does it want its audience to do about it? Clear messaging should educate, inspire, and move its recipients to action regarding the organization’s mission.

- **Selection of Media** – Based on the internal and external analysis and comprised of the messaging outcomes, the organization should identify the specific media to be used to in order to maximize each of the five modes of communications: electronic, visual, audio, print, and face-to-face.\(^8\) In addition to the application of “media” as modes of communications (website, internet, podcasts, brochures, etc.), the plan should include the use of media outlets (local and national television, newspapers, magazines, radio, etc.)

- **Establishing Benchmarks** – The plan should include strategic goals and objectives that determine the success of each outreach effort. What will the measures of success be? (for example, number of event attendees? number of petition signers? number of social media “likes” and “shares?”) Setting and evaluating benchmarks will help the plan to effectively grow the organization – and grow with the organization.

- **Plan Ratification and Distribution** – The final plan document should include the organization's mission and vision statements, an introductory summary of each of the planning outcomes, a statement of the benchmark objectives, a budget reflecting allocation of existing resources and resources to be pursued and developed, and a timeline for implementation. Once finalized, the plan should be distributed to key staff and stakeholders. The entire plan – or subsets of the document, at the chief executive’s discretion – should be distributed to the entire staff.\(^9\)

---


\(^8\)Patterson and Radtke, 2009.
It is no accident that the process cycles for resource development and communications are nearly identical – one is about fundraising, the other is about friend-raising. Neither can be fully successful without the other. Many organizations place the communications and development roles under the same management to ensure mutual support of each. The communications planning and execution process is often linked to the organization’s development and fundraising process. It should also reflect the meaningful involvement of any volunteer management activities to achieve and sustain constituent engagement.

**Working with Social Media**

![SOCIAL MEDIA](image)

A group of mobile and internet-based applications that allow the creation and exchange of user-generated content.

The most important phrase in this definition of social media is “exchange of user-generated content.” If organizational communications were historically a one-sided monologue – and engaging the public is essentially a dialogue – the advent of social media begins a virtual partnership, with individuals and other organizations sharing the task of analyzing and responding to mission-related issues, policies, and events. The social media user is neither primarily an information recipient, as in standard communications, nor primarily an information transmitter, as with successful public engagement. With social media platforms, the user becomes an active collaborator and the empowerment of the user community is the greatest factor in the platform’s appeal. *(See Attachment M “Social Networking Policy”)*

Benefits of Establishing a Social Media Network

- Reduces the demands on staff for disseminating organizational information by making the answers to frequently asked questions available to the public at large
- Exponentially raises the organization’s public profile by engaging the community in promoting programs, events, and activities
- Allows rapid response to emergent situations and circumstances
- Demonstrates public support for the organization by building a community of “friends,” “followers,” and “likes”

With millennials leading the charge as today’s activists, every nonprofit must consider seriously the surging use of social media by 18 to 34-year old and the appropriate use of these platforms in reaching its audience and constituents. In a recent report by the Pew Research Center, in 2016, 68 percent of online adults reported using Facebook, 25 percent using LinkedIn, 26 percent using Pinterest, 21 percent using Twitter, and 28 percent using Instagram. In the same report, 86% of those between the ages of 18 and 29, 80% of those between 30 and 49, 64% of those between 50 and 64, and 34% of those over the age of 65 use at least one social media site.

Find more information on social media usage from the Pew Research Center’s Social Media Fact Sheet: [http://www.pewinternet.org/fact-sheet/social-media/](http://www.pewinternet.org/fact-sheet/social-media/)

---

Before you begin:

- **Answer “Yes or No”**
  
The first question to be answered is whether an organization’s mission, programs, and constituency warrant social media engagement beyond a website, and whether the organization’s current resources can establish or support that engagement. While every organization should have some digital or Internet presence, not every organization is suited to an active social media component. For example, an organization serving a constituency unlikely to have access to the Internet or engage in social media may answer this question differently from one serving a watchdog function on current public events.

- **Answer the question “Why?”**
  
Identify the top two or three goals for engaging in social media that your organization wishes to achieve (you can also use the “Benefits of a Social Media Platform” list provided here to help you identify potential benefits that may not have been considered previously.) Once the goals for social media outreach have been identified, these goals should drive the decisions as to the platforms in which the organization should engage. This analysis should also include objective means of determining whether the named goals are being effectively achieved.

- **Who is in control?**
  
There is no way to control opposing viewpoints of the conversation in the interactive world of social media – in fact, it is best not to try. While it is possible to establish an approval process for comments, then the question becomes “who will manage that process timely and effectively?” The board should be directly involved in the analysis and decision-making regarding these issues, as it is responsible addressing any legal, moral, or financial liabilities that may arise from participating in un-vetted public interactions.

**Social Media Platforms**

There are numerous social platforms available, with more being introduced all the time. It takes significant time and activity to build a community through any social medium, so focus first on the one or two platforms best suited to achieve your immediate goals and maximize your existing resources. You can engage in additional platforms after you have built some momentum in your primary media.

**Facebook** – An online social networking service. Users create a personal profile, add other users as “friends,” “like” organization’s pages, and exchange messages, images, and information. Users may join common-interest user groups and categorize their friends into lists. According to Facebook’s newsroom website, there were 1.28 billion daily active users on average for March 2017.10 A Facebook page is now an important social medium for any organization.

**Twitter** – An online social networking and microblogging service that enables users to send and read "tweets"—short text messages limited to 140 characters. Users access Twitter through a website interface or mobile device application (an “app.”) Twitter runs a not-too-distant second to Facebook in the social media race for utility and influence.

---

and is particularly effective in the immediate distribution of a real-time message in emergency or time-sensitive situations.

**YouTube** – A video-sharing website on which users can upload, view, and share videos. The site displays a wide variety of user-generated video content, including video clips, TV clips, music videos, and amateur content such as video blogs or “vlogs,” short original videos, and educational videos. Organizations whose missions embrace the visual or performing arts or transformational services should consider this an essential tool. YouTube also holds great utility for the posting of educational videos, presentations, event and project documentation, and other visual media for any organization.

YouTube offers special services for videos posted by certified nonprofits, including donation buttons, event streaming, video annotations, and public engagement overlays. View more here: [http://www.youtube.com/nonprofits](http://www.youtube.com/nonprofits).

**Blogging** – A “blog” (contraction of the phrase “web log”) is a discussion or informational site consisting of individual "posts" or entries. While most often the work is by an individual, "multi-author blogs" (MABs) from organizations are on the rise and are supported by other social media platforms.

Other social media websites that your organization may want to explore include Instagram and Pinterest – both photo-based sites, LinkedIn – a professionally-oriented social media service, and Snapchat – a mobile application for image messaging. While not all social media sites may fit your organizational communication needs, it is beneficial to keep informed on the newest communication outlets.

**Mobile Applications**
In 2017, 71% of all “digital minutes” are spent via mobile devices including smart phones and tablets and the number of global users of mobile devices have surpassed those using desktops. It is no long a question of if to engage mobile users but how.11

It is no surprise that mobile is here to stay. A nonprofit’s decision to embrace mobile technology means more than just having a responsive website, it is about offering your community an additional, even customized way to receive information. But what does it mean to “go mobile?” Leah Readings from [Capterra’s Nonprofit Technology Blog](http://www.capterra.com/technology/blog) identifies four categories of mobile presence:

- **Mobile Web.** Ensuring your website, copy, and online content are optimized for access on mobile devices
- **Mobile Messaging.** Communicating with your community using text and instant messaging
- **Mobile Fundraising.** Offering your community ways to make financial contributions through their mobile devices via text or mobile-optimized donation forms

---

• **Mobile Apps.** Developing a downloadable mobile application so your community can easily access your organization’s programs and content.

If your organization is considering increasing its mobile presence, start by developing a mobile strategy that considers the different audiences you would like to engage and how each of these groups typically prefer to receive information. You may want to start thinking about how your regular copy and visual communications will be received on a variety of mobile devices. If you’re interested in developing a full-fledged mobile app that can be downloaded onto a mobile device, you may wish to consult a professional developer. Additionally, there are a variety of convenient online tools for non-professionals to build and release quality apps for a substantially lower cost.

**Beginning with Social Media**

- **Check Out the Competition:** Look at what other organizations with similar or competing missions are doing. Try to employ what impresses you without duplicating it, and make notes to avoid what discourages your interest.

- **Put your Best Food Forward:** If the selected social medium allows for the personalization of your organizational presence, take full advantage of that option. The more compelling and unique your digital presence, the more attractive and engaging it will be to potential followers. Develop a “look and feel” for your visual media and a “tone and feel” for your verbal media that truly reflect your organization– and be consistent with these profiles.

- **Assign Responsibility:** Effective use of social media takes consistent effort, preferably with some historical memory. If possible, responsibility for populating and monitoring the organization’s social media platforms should be assigned to a single person who can devote a meaningful amount of time to the task – not "spare time", but full-time or part-time. This person does not have to do everything, but they must be responsible for ensuring that regular updates; responses to posts, messages, and inquiries; and real-time responses to emergent occurrences are accomplished through support from other staff or volunteers.

- **Give and Take:** For those medias that allow for links and connections, such as Facebook and YouTube, reach out to other organizations with which you partner or wish to partner and establish mutual platform links. This gives you a jumpstart on building your own community while increasing your value as an information resource for your own followers.

**Enhance your Existing Social Media Platforms**

- **Narrow your focus:** Create an additional group or groups based on one or more aspects of your programs and services and establish a presence for them on your platforms. A narrower or more specific focus can potentially increase both the number of viewers and followers and their level of engagement. You may also be able to become an “official sponsor” of an existing and active group comprised of your service constituency – check your platform’s policies and procedures to find out if you can and how.

- **Ask an expert:** Sometimes looking at the same thing with a new and informed eye can reveal easy ways to enhance what you are already doing and suggest what more you can do.

---

This can be a professional consultant and/or a member of your community who is a very active participant in social media.

- **Pull your friends closer:** Send an e-mail to your existing community specifically inviting them to connect with your organization’s social media platform(s.)
- **Ideally, update the content of social media daily:** If this is not the case for your organization, determine if and how it can become the case or what other frequency is feasible.
- **Add a blog, if you do not have one already.** You can feature original articles or – if your resources are limited and there is an existing blogger harmonious with your focus and context – invite him or her to feature that blog on your site or write blogs for you.
- **Always provide an avenue for donating time, energy, and money to the organization in your social media platforms.**
- **Always provide an opportunity to get involved in the events and activities announced in your platform:** Be sure to report on the success of an event, project, or program after the fact to spark interest in future opportunities to participate.

**A Special Note:**

Too often organizations emphasize using social media to acquire as many “friends” and “followers” as possible. While the number of subscribers can reflect the organization’s popularity, the emphasis should be on driving conversations about the issues addressed by the organization’s mission that are important to the community and facilitating their engagement in those conversations. One may need not visit your facility or an in-person program to advance your mission. Serving as an informational resource is also an important function.

**Selected Resources for Administrative Policies**

**Books and Articles**


**Websites**

*Crisis and Disaster Planning American Red Cross*  
http://www.redcross.org/prepare

*ASAE*  
http://www.asaecenter.org/Search/search.cfm?Query=crisis+plan&x=0&y=

*FEMA*  
https://www.fema.gov/plan-prepare
Nonprofit Risk Management Center
http://www.nonprofitrisk.org/consulting/risk-assess.shtml

"Preparedness Planning for Businesses/Organizations"
http://www.ready.gov/business

“Continuity of Operations Plan (COOP) for Non-Profit Human Services Provider” A template to guide an organization through the steps needed to begin the process of developing a comprehensive COOP plan for the organization

“Disaster Preparedness and Recovery Plan,” Council on Foundations: Very comprehensive and helpful planning guide for disasters that includes interactive portions and advice as to determining a plan of action and recovery plans.

“Elements of Disaster Planning” Very helpful checklist created by Emergency Network of Los Angeles.

http://www.techsoup.org/disaster-planning-and-recovery

“Where can I learn more about disaster planning for my nonprofit?” http://www.grantspace.org/Tools/Knowledge-Base/Nonprofit-Management/Sustainability/Disaster-planning

Additional Tools Specific to Programs and Populations Served
Disability Prepared (Research and Training Center on Independent Living (RTC/IL), University of Kansas - Best of Best Practices website)
http://www2.ku.edu/~lsiprepared/

Disaster Planning for Animals (Humane Society of America website)
http://www.humanesociety.org/about/departments/disaster_preparedness.html#.Uw4k4M5kXkc

Preparing for Disaster for People with Disabilities and other Special Needs (Red Cross Booklet)
http://www.redcross.org/images/MEDIA_CustomProductCatalog/m4240199_A4497.pdf

Crisis Communication

“7 Steps for Social Media Crisis Management”
http://www.psfk.com/2013/08/social-media-crisis-management.html#!/x9j0f


“The Socially Responsible Role of Social Media in Crisis Management”  
http://www.technewsworld.com/story/77439.html


Information Technology

Web 2.0 Governance Policies and Best Practices  

Implementing a Bring Your Own Device Policy: What Your Nonprofit Needs to Know  

Communications and Social Media

Sample Policies
Web 2.0 Governance Policies and Best Practices  

The Nonprofit Social Media Policy Workbook, ideal ware (April 2012)  

Communications Related Websites

http://www.slideshare.net/search/slideshow?searchfrom=header&q=online+volunteer+recruitment&ud=any&ft=all&lang=*&sort=  
Slideshare.net has several instructional videos on using the internet and social media to engage the public, and recruit volunteers

See, Say, Feel, Do: Social Media Metrics that Matter, Fenton Communications

Attachments

Crisis and Disaster Planning


Information Technology

Communications and Social Media
• Attachment M: Social Networking Policy – reprinted with permission of The Arc Baltimore.
• Attachment N: Essential Communications Tools – from Generate Buzz! Strategic Communication for Nonprofit Boards, Sally Patterson, BoardSource 2011. Reprinted with permission of Sally J. Patterson.
Attachment A
Crisis and Disaster Planning

Sample Plan Introduction
(Can also be called: Crisis, Disaster, Contingency, or Continuity Plan)

The purpose of this document is to identify and address the critical factors that may affect (THE NONPROFIT) in the event of a national, regional, or local emergency, disaster, or another unexpected event.

Our priorities are to:
- Secure the safety and well-being of all (THE NONPROFIT)’s clients and staff
- Protect our business property
- Safeguard our assets
- Provide an operational guideline for recovery
- Where possible, assist other organizations and individuals in responding to the crisis
- Add your own

Principles that guide our actions:
- Open and continuous communication with our staff, board members, and clients
- Respect for privacy and dignity of all people
- Quick action and response
- Support for those directly affected
- Add your own

We recognize that while crisis/disaster/contingency planning can address some likely events, there are other emergency situations that cannot be predicted. Therefore, (THE NONPROFIT) has designated a response team to provide the structure, policies, and principles for action in the event of an emergency.

Additional items to consider:
- Cross-train staff so that your organization will be able to fully function even with lower numbers of staff members present to complete the work of your organization
- Ensure that you have the information technology to support employees who wish to be able to work from home or who may need to work from home or at remote locations.
- Consider instituting flexible workplace and leave policies. There may be additional need in cases where there are school closures if parents need to stay home to care for children, or if employees are sick, caring for ill family members, or otherwise unable to work due to issues related to the disaster situation.
Attachment B
Crisis and Disaster Planning

Sample
Roles and Responsibilities of Disaster/ Crisis Response Team

Responsibilities of (THE NONPROFIT)’s Response Team

(THE NONPROFIT)’s Response Team is comprised of designated members of (THE NONPROFIT)’s Senior Management staff and at least one member of the Board of Directors.

The following staff positions serve on the Response team (select your own):
• President/CEO/Executive Director
• Vice Presidents/Program Directors
• Director of Human Resources
• Director of Administration
• Director of Communications
• Director of Volunteers
• Board Member(s)
• Add your own

The team is responsible for the development, periodic review, and implementation of this plan. In the event of an emergency, (THE NONPROFIT)’s Response Team will meet (digitally or in person) to assess the situation and develop a specific plan of action in response to an emergency.

Response Team Objectives/Roles

In the event of an emergency, crisis or other disaster, the (THE NONPROFIT)’s Response Team’s tasks are:

1. Information Gathering and Assessment
   • Gather information quickly from at least (three) reliable sources
   • Gather all relevant and accurate details
   • Assess the need for immediate intervention and mobilize resources

2. Immediate Actions
   • Secure the safety of people and property
   • Evaluate damage and possible consequences
   • Set up alternative plans, if needed, to continue regular business operations
   • Minimize the impact and loss
   • Return to normal operations as soon as possible
3. Communication
   • Respond promptly to multiple audiences (staff, volunteers, board, families, clients, vendors, funders, partners, media, general public)
   • Organize a telephone network to inform people of necessary information
   • Calm fears, stop rumors, reduce uncertainty
   • Plan for a public statement/press release
   • Ensure the privacy and dignity of all people
   • Protect (THE NONPROFIT)’s credibility and reputation

4. Assessment
   • Conduct post-crisis evaluation
   • Revise plan as needed

(Document the following information and make it available to all members of the response team and other key staff and board members.)

<table>
<thead>
<tr>
<th>Position Title (Staff &amp; Board)</th>
<th>Name</th>
<th>Location/Telephone/e-mail</th>
<th>Primary Roles on the Response Team</th>
<th>Back Up Person</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Attachment C
Crisis and Disaster Planning

Sample Risk Assessment Worksheet

Examples of events that could disrupt business:
- **Natural Disasters** – hurricane, earthquake, flood, fire
- **Civil Disruptions** – terrorism, riot, police action, bomb threat, threat of war
- **Criminal Activity** – burglary, workplace violence
- **Technology Emergency** – computer virus, corruption of critical data
- **Health Emergency** – infectious disease, epidemic, pandemic, contamination
- **Travel Emergency** – airplane/train accident, shutdown of major transportation services
- **Loss of Essential Members** – serious illness or death
- **Loss of Access to Workplaces** – office building or community emergency
- **Loss of Intellectual Capital** – loss of information and intuitive processes
- **Loss of Financial Capital** – fraud, unanticipated contract loss, banking system shutdown, loss of major funder or donor

Steps in Risk Assessment
1. **Review** the list of possible events and add to it, as needed
2. **Identify** specific scenarios/situations that are most relevant to your program focus, location, and community – for example, is your area prone to hurricanes or tornadoes or earthquakes? Do your clients and staff rely on public transportation to get to your location? Is your website the principal entry point for people accessing your services? Can you provide your programs only in specific location(s)?
3. **Prioritize** the potential crises to focus your need for planning and action
4. **Answer** these questions:
   - How likely is each event/crisis to occur?
     - Within 1 to 2 years
     - Not very likely
     - Unable to predict
   - What is the anticipated duration of disruption?
     - Short term
     - Long term
     - Ongoing
   - What is the potential impact on the organization should this occur?
     - Minimal
     - Major
   - Who would be most affected?
     - Your staff
     - Your clients
5. **Summarize** your assessment
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>TYPES OF EVENTS ADD YOUR OWN EXAMPLES</th>
<th>PRIORITIZE FOR YOUR ORGANIZATION (1...10)</th>
<th>LIKELIHOOD</th>
<th>POTENTIAL IMPACT</th>
<th>WHO WOULD BE MOST AFFECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Disasters</td>
<td>hurricane, earthquake, flood, fire</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Civil Disruptions</td>
<td>terrorism, riot, police action, bomb threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criminal Activity</td>
<td>burglary, workplace violence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Emergency</td>
<td>computer virus, corruption of critical data, telecom interruption or shutdown</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health Emergency</td>
<td>infectious disease, epidemic, pandemic, contamination</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Travel Emergency</td>
<td>airplane/train accident, shutdown of major transportation services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of Essential Members</td>
<td>serious illness or death</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of Access to Workplaces</td>
<td>office building or community emergency</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of Intellectual Capital</td>
<td>loss of information and intuitive processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of Financial Capital</td>
<td>fraud, unanticipated contract loss, banking system shutdown, loss of major funder or donor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add your own</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Attachment D**

**Crisis and Disaster Planning**

**Sample**

**Continuity Plan Worksheet**

**Business Continuity Planning addresses the following areas:**

- **Preparation** – actions taken prior to disaster, crisis event, emergency
- **Response** – procedures and steps done immediately after an emergency or interruption to the business
- **Recovery/Restore** – steps taken to restore some functionality so that some level of business can be offered to customers while restoring the organization to its original status prior to an interruption

### Sample Continuity Plan

**Enter your own information**

<table>
<thead>
<tr>
<th>Event</th>
<th>Preparation</th>
<th>Response</th>
<th>Recovery/ Restoration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Natural Disasters</strong></td>
<td><em>Office evacuation plan</em></td>
<td><em>911</em></td>
<td><em>Business insurance</em></td>
</tr>
<tr>
<td></td>
<td>*Office smoke detectors and fire extinguishers</td>
<td><em>Contact staff and customers</em></td>
<td><em>Continue operations from alternate locations</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><em>Reschedule activities</em></td>
</tr>
<tr>
<td><strong>Civil Disruptions</strong></td>
<td><em>Office evacuation plan</em></td>
<td><em>911</em></td>
<td><em>Continue business operations from alternate locations</em></td>
</tr>
<tr>
<td></td>
<td><em>Designated alternate locations</em></td>
<td><em>Contact staff</em></td>
<td><em>Reschedule activities</em></td>
</tr>
<tr>
<td></td>
<td><em>Remote Access</em></td>
<td><em>Contact customers</em></td>
<td></td>
</tr>
<tr>
<td><strong>Criminal Activity</strong></td>
<td><em>Preventative measures</em></td>
<td><em>911</em></td>
<td><em>File business insurance claim</em></td>
</tr>
<tr>
<td></td>
<td><em>Business insurance</em></td>
<td><em>Contact police and file a report</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>EAP</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Technology Emergency</strong></td>
<td><em>Backup of computer systems housed off-site</em></td>
<td><em>Contact tech support vendors</em></td>
<td><em>Restore from back up data</em></td>
</tr>
<tr>
<td></td>
<td><em>Restoration of backups tested regularly</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Password and virus protection software</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Multiple communication methods</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Health Emergency</strong></td>
<td><em>Alternate locations</em></td>
<td><em>Review travel records for the last 2 to 4 weeks for potential vectors.</em></td>
<td><em>Work from home office locations. Ensure remote work options are in place for as many team members as feasible</em></td>
</tr>
<tr>
<td></td>
<td><em>Telecommuting</em></td>
<td><em>Assess the situation and explore travel alternatives</em></td>
<td><em>Send alternate staff</em></td>
</tr>
<tr>
<td></td>
<td><em>Remote access to data</em></td>
<td><em>Contact staff</em></td>
<td><em>Reschedule, modify (potentially involving detection or monitoring of participants), or cancel activities, especially gatherings of large numbers of people</em></td>
</tr>
<tr>
<td></td>
<td><em>Liberal leave</em></td>
<td><em>Reschedule activities</em></td>
<td><em>Follow World Health Organization, Centers for Disease Control, National</em></td>
</tr>
<tr>
<td></td>
<td><em>Maintain list of where employees have traveled for business travel</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Create policies around non-punitive sick leave</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td>Preparation</td>
<td>Response</td>
<td>Recovery/ Restoration</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Travel Emergency</td>
<td>*Phone tree&lt;br&gt;*Multiple methods of communication&lt;br&gt;*EAP</td>
<td>*Secure safety of staff&lt;br&gt;*Explore travel alternatives&lt;br&gt;*Contact customers</td>
<td>*Arrange for possible completion of activities by other staff&lt;br&gt;*Reschedule activities</td>
</tr>
<tr>
<td>Loss of Essential Members</td>
<td>*Succession planning&lt;br&gt;*Cross training&lt;br&gt;*EAP</td>
<td>*Contact board and staff&lt;br&gt;*Implement succession plan&lt;br&gt;*Share responsibilities</td>
<td>*Hire interim or acting staff or promote to fill position</td>
</tr>
<tr>
<td>Loss of Access to Workplaces</td>
<td>*Multiple locations/Telecommuting&lt;br&gt;*Business insurance&lt;br&gt;*Inventory of property updated annually</td>
<td>*Work from multiple locations&lt;br&gt;*Contact office management company</td>
<td>*Relocate office location if necessary</td>
</tr>
<tr>
<td>Loss of Intellectual Capital</td>
<td>*Succession planning&lt;br&gt;*Cross training&lt;br&gt;*Desk manuals&lt;br&gt;*Leadership development&lt;br&gt;*Information sharing</td>
<td>*Contact staff and customers&lt;br&gt;*Recreate loss of information and processes&lt;br&gt;*Share responsibilities</td>
<td>*Hire or promote to fill position</td>
</tr>
<tr>
<td>Loss of Financial Capital</td>
<td>*Cash reserves of at least six months&lt;br&gt;*Line of credit&lt;br&gt;*Internal controls</td>
<td>*Contact staff&lt;br&gt;*Contact customers and vendors</td>
<td>*Contingency plan and budget are implemented</td>
</tr>
</tbody>
</table>
Attachment E
Crisis and Disaster Planning

Sample
Emergency/ Crisis Communication Plan

Priority Audiences (Define)
• Staff and their families, volunteers, and board members
• Clients
• Funders and key business partners
• Media and general public

Advance Preparation/Ongoing
• Maintain up-to-date contact lists, accessible to several people in multiple locations
• Maintain current staff schedule and travel information, accessible to several people in multiple locations
• Maintain a media contact list, accessible to several people in multiple locations
• Establish a “telephone” tree system in advance

Immediate Action
• Define the message to be communicated and whom to contact for additional information
• Make personal phone calls, whenever possible, to staff and their families, and the board of directors
• Send e-mail messages to other audiences
• Post press release or other messages on (THE NONPROFIT)’s web site and other social media
• Send press release via e-mail

Sample Media Policy
(THE NONPROFIT) is committed to open and honest communication regarding the release of information. (THE NONPROFIT) will protect the privacy of personal information of its clients, employees, volunteers, and board members. (THE NONPROFIT) will not comment on individual situations, but will present a statement of organizational position as needed.

If an occasion arises that requires media contact:
• Executive director, with advice from (THE NONPROFIT)’s Response Team, determines if a press release is needed and what points are to be covered in the press release.
• Director of Communications drafts the press release. (THE NONPROFIT)’s executive director and Response Team reviews the release.
• Executive director and Response Team decide the audiences for the release – clients, staff, board members, partners, funders, and media.
• Director of Communications distributes the press release through relevant social media
• All media inquiries are referred to (THE NONPROFIT)’s executive director. If (THE NONPROFIT)’s executive director is not able to be reached, all media should be referred to (THE NONPROFIT)’s board chair.
Director of Communications prepares all staff for media calls – how to respond to and refers callers.
Attachment F  
Information Technology

Sample  
Technology Policy  
(and Privacy Policy for Users)

Purpose:

(THE NONPROFIT) seeks to effectively manage our technology and computer systems and guide the use, maintenance and security of the hardware, software, and data. Employees are responsible for ensuring that the procedures and policies outlined here are followed.

Use:

Using computer equipment (collectively, hardware and software) requires care because of its fragility, susceptibility to viruses and malware, and high cost. Access to the equipment should thus be strictly reserved to (THE NONPROFIT) employees only (and to certain interns, volunteers, and members under the supervision of staff.) Those employees who need additional training on hardware or software to complete their job duties will be given an orientation by upon hire and upon request. At least one employee will be trained in handling minor maintenance of software, hardware, and accessories at the office (projectors, keyboards, external hard drives, etc.)

a. **Acquisition:** Computers are purchased based on the technical specifications and price of the machine, in line with budgeted IT expenditures for the year. Computers should have at least 4GB of RAM, Intel i3 processor or higher, 250GB or more hard drive space available, and at least a 15-inch screen, (add your own specifications) unless requested otherwise.

b. **Disposal:** After a maximum of five years, computers should be repurposed as a spare laptop or donated, and replaced with a new computer.

c. **Acceptable Use:** (THE NONPROFIT) equipment should only be used for purposes related to completing your job duties for (THE NONPROFIT.) This includes but is not limited to laptops, desktops, projectors, printers, data storage, etc. Consultants, volunteers (including interns,) and members should seek prior permission of an employee before using the office equipment.

d. **Computer Maintenance:** Computers should be completely shut down at least once a week. Employees are free to complete updates for familiar programs. Updates that look unfamiliar may be potentially malicious and may affect the computer’s operating system, and should be forwarded to IT support. Quarterly, by appointment, desktops and laptops are to be cleaned, have dust removed from fan, have updates completed, and other
computer maintenance. Laptops should always be placed on a hard surface during use. This is to prevent the fan from over-heating due to dust accumulation or lack of air circulation.

e. **Accessory Equipment:** Tech equipment (including projectors, laptops, webcams, speakers, etc.) should be signed out and signed back in upon return. This accessory equipment is only to be used by staff or under the supervision of staff. Staff who are unable to operate various tech equipment should contact IT support for training.

f. **Internet Connection:** Staff should connect to the Wi-Fi network using the password. Guests to the office should connect to the Wi-Fi network using the password.

g. **Cloud Storage:** Staff should save work documents to the cloud folder located on their computer’s desktop. This will ensure that a copy of the document is accessible, up-to-date, and backed up. Please contact IT support if you are unable to find your cloud folder.

h. **Software Setup for All Employees:** All employees’ and spare computers upon purchase and assignment, should be set up with the following software:
   - Microsoft Office 365 Nonprofit Business Premium
   - Box Plugins (Box Sync, Box Edit, Box for Office 365, dav.box.com)
   - Adobe Acrobat Reader
   - Google Chrome, Internet Explorer, and Firefox
   - Symantec Antivirus software
   - Centrastage software
   - Cute PDF writer
   - Printers drivers
   - Organization fonts – Trajan Pro and Optima LT and SFX fonts – Times New Roman and Futura Medium.
   - Desktop shortcuts

Upon hire, all employees will be set up with:
   - Email address
   - Phone extension
   - Add to all staff email distribution list in Office 365
   - (add your own)

i. **User Training:** Twice a month, there will be one-hour trainings scheduled on various topics related to (THE NONPROFIT) software and hardware usage. Training topics will be determined at the previous staff meeting. Trainings will be completed over Adobe Connect and will be recorded. In addition, staff will have regular access to other training materials.

**Security**
a. **Ownership and Protection of Data:** (THE NONPROFIT) proprietary data (data contained in our CRM system and on our cloud server) should only be used for purposes related to (THE NONPROFIT.) Employees and volunteers should refer to their employee or volunteer handbook for further instruction about what information is considered private and confidential. In addition, employees are responsible for ensuring that the Privacy Policy for Users publicized to our members is followed (see attachment.) Data should not be released outside of the organization without the consent of a supervisor or in the absence of a specific Memorandum of Understanding regarding the appropriate use of the data.

b. **Permissions:** A system will be put in place to ensure that only necessary permissions are granted to employees to access, view, edit, copy, and delete organization data.

c. **Document Destruction and Retention:** Employees should reference the document destruction and retention policy located in the employee manual to determine what data is required to be retained and/or destroyed at least annually.

d. **Anti-Virus Software:** To safeguard computers from viruses, antivirus software has been installed on the computers and should be updated regularly (at a minimum, during quarterly maintenance by IT support.) Virus/system scans will be run regularly. Staff are encouraged to install Windows system updates when prompted. If staff are unsure if an update should be completed, they should contact IT support. Updates that make changes to the operating system should be checked with IT support first.

e. **Personal Accountability:** To safeguard computers from viruses, malware, and other data breaches, please be vigilant of email attachments from unknown senders and downloadable content from unfamiliar websites. If content seems suspicious, refrain from opening content and contact IT support. Employees and volunteers are responsible for understanding the risks to data security. Unattended workstations, poor passwords, sharing passwords, and lost laptops are the most common causes of security breaches.

f. **Backup:** There should be at least two backups of all important documents. One copy should be kept in the cloud. The other copy will be backed up weekly to an external hard drive through regularly scheduled backups. A new backup is created every Friday evening at 7:00 PM.

g. **Passwords:** To ensure the creation of sufficiently encrypted passwords, please include a combination of Upper and lowercase letters, numbers, and symbols. See example below. Passwords should be added to the Password File located in the Box folder. ex. Password1!  

**Outsourced Technology Support**

We currently outsource our tech support (add organization.) To place a service ticket please complete the following steps: (add tech support specific steps)
Attachments and Related Policies

Attached: Privacy Policy for Users


Approved by (THE NONPROFIT) board on (date.)

Attachment: Privacy Policy for Users

(THE NONPROFIT) places a high priority on protecting your privacy. This privacy policy was created to demonstrate (THE NONPROFIT)’s firm commitment to the privacy of our members and website users. This policy explains what types of information is collected by (THE NONPROFIT) website, and how this information is used.

What Information is Collected

(THE NONPROFIT) collects personally identifiable information, such as your e-mail address, name, home or work address or telephone number. (THE NONPROFIT) also collects anonymous demographic information, which is not unique to you, such as your ZIP code, age, gender, preferences, interests and favorites.

There is also information about your computer hardware and software that is automatically collected by (THE NONPROFIT.) This information can include: your IP address, browser type, domain names, access times and referring Website addresses. This information is used by (THE NONPROFIT) for the operation of the service, to maintain quality of the service, and to provide general statistics regarding use of the (THE NONPROFIT) Website.

Please keep in mind that if you directly disclose personally identifiable information or personally sensitive data through (THE NONPROFIT) public message boards, this information may be collected and used by others.

Note: (THE NONPROFIT) does not read any of your private online communications.

(THE NONPROFIT) encourages you to review the privacy statements of Websites you choose to link to from (THE NONPROFIT) so that you can understand how those Websites collect, use and share your information. (THE NONPROFIT) is not responsible for the privacy statements or other content on Websites outside of the (THE NONPROFIT).

How Your Information May Be Used

(THE NONPROFIT) collects and uses your personal information to operate (THE NONPROFIT) Website and deliver the services you have requested. (THE NONPROFIT) also uses your personally identifiable information to inform you of other products or services available from (THE NONPROFIT) and its affiliates. (THE NONPROFIT) may also contact you via surveys to conduct research about your opinion of current services or of potential new services that may be offered.
Nonprofits does not sell, rent or lease its customer lists to third parties without express permission. (THE NONPROFIT) may, from time to time, contact you on behalf of external business partners about an offering that may be of interest to you. In those cases, your unique personally identifiable information (e-mail, name, address, telephone number) is not transferred to the third party. In addition, (THE NONPROFIT) may share data with trusted partners to help us perform statistical analysis, send you email or postal mail, provide customer support, or arrange for deliveries. All such third parties are prohibited from using your personal information except to provide these services to (THE NONPROFIT,) and they are required to maintain the confidentiality of your information.

(THE NONPROFIT) does not use or disclose sensitive personal information, such as race, religion, or political affiliations, without your explicit consent.

(THE NONPROFIT) keeps track of the Websites and pages our customers visit within (THE NONPROFIT), to determine what (THE NONPROFIT) services are the most popular. This data is used to deliver customized content and advertising within (THE NONPROFIT) to customers whose behavior indicates that they are interested in a subject area.

(THE NONPROFIT) Websites will disclose your personal information, without notice, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on (THE NONPROFIT) or the site; (b) protect and defend the rights or property of (THE NONPROFIT); and, (c) act under exigent circumstances to protect the personal safety of users of (THE NONPROFIT), or the public.

Use of Cookies
The (THE NONPROFIT) Website use "cookies" to help you personalize your online experience. A cookie is a text file that is placed on your hard disk by a Web page server. Cookies cannot be used to run programs or deliver viruses to your computer. Cookies are uniquely assigned to you, and can only be read by a web server in the domain that issued the cookie to you.

One of the primary purposes of cookies is to provide a convenience feature to save you time. The purpose of a cookie is to tell the Web server that you have returned to a specific page. For example, if you personalize (THE NONPROFIT) pages, or register with (THE NONPROFIT) site or services, a cookie helps (THE NONPROFIT) to recall your specific information on subsequent visits. This simplifies the process of recording your personal information, such as billing addresses, shipping addresses, and so on. When you return to the same (THE NONPROFIT) Website, the information you previously provided can be retrieved, so you can easily use the (THE NONPROFIT) features that you customized.

You may accept or decline cookies. Most Web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. If you choose to decline cookies, you may not be able to fully experience the interactive features of the (THE NONPROFIT) services or Websites you visit.

Security of your Personal Information
(THE NONPROFIT) secures your personal information from unauthorized access, use or disclosure. (THE NONPROFIT) secures the personally identifiable information you provide on
computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. When personal information (such as a credit card number) is transmitted to other Web sites, it is protected using encryption, such as the Secure Socket Layer (SSL) protocol.

**Changes to this Statement**

(THE NONPROFIT) will occasionally update this Statement of Privacy to reflect company and customer feedback. (THE NONPROFIT) encourages you to periodically review this Statement to be informed of how (THE NONPROFIT) is protecting your information.

**Contact Information**

(THE NONPROFIT) welcomes your comments regarding this Statement of Privacy. If you believe that (THE NONPROFIT) has not adhered to this Statement, please contact (THE NONPROFIT.) We will use commercially reasonable efforts to promptly determine and remedy the problem.

An Acceptable Use Policy (AUP) is a document that explains how technology should be used by staff, board, and other volunteers of an organization. The purpose of the AUP is to prevent the use of organization-owned technology and/or information for irresponsible, illegal, or abusive activity. There is a wide variety of theories on how best to construct an effective AUP. Some organizations believe in strict policies that prohibit the use of organization-owned computers for personal matters. Others believe that the increased risk of allowing reasonable personal use is offset by enhanced morale and productivity. There is, arguably, no one way to go about crafting an AUP, and your approach should be guided by your organization’s own philosophy and culture.

**Elements of an AUP**

The topics covered in an AUP vary, but below are a few of the most common:

- E-mail policies and procedures
- Downloading files
- Internet use
- Social networking
- Security practices
- Hardware/Software specifications
- File Management

**Drafting the AUP**

There are a few simple things to keep in mind while drafting the AUP.

*Skip the Legal Talk*

Your AUP should be aimed at getting staff, board, and other volunteers to understand how you expect your technology to be used. If it is written with the stiff, jargon-filled language of legal experts, people won’t be able to read it. If people cannot read it, why bother writing it?

*Practice Consistency*

Strive to make your document as consistent as possible. If you want people to follow your guidelines, be clear about those guidelines. Do not write “violators will be immediately terminated” in one section and “violators will receive a gentle warning” in another. If the AUP contradicts itself, users are not going to respect its guidelines.

*Use Appropriate Language*

Too often, policy documents do not take a reader-centered approach. This can create an AUP that contains cold, offensive, or demeaning language. It is important to consider how the reader will respond to the content. Staff members, volunteers, and board
members are professional adults and deserve to be treated as such. To ignore this fact can lead to loss of morale and damage productivity. Using appropriate, user-centered language is especially necessary when introducing an AUP into an already established work environment. Users who are used to a status quo may see the introduction of an AUP as a sign of undue control or as an indication that they are not performing adequately.

*Explain Prohibitions*

Along with using appropriate language, an AUP should also contain sound reasoning. Instead of just listing the actions that are prohibited, explain why the regulation is in place. This will increase the likelihood of compliance by helping the reader understand your viewpoint.

A very comprehensive AUP from the University of Chicago can be accessed here: [http://nsit.uchicago.edu/policies/eaup/](http://nsit.uchicago.edu/policies/eaup/)

For small organizations, hiring an IT consultant can be a daunting task, one made more difficult if the organization is not familiar with technology or the scope of the IT project is unclear. The following steps will insure you find a quality consultant that meets your needs.

Step 1: Define project objectives

Decide on a budget and timeline for the desired project. It isn’t essential that you know exactly what you need (that is the consultant's job after all), but you should know what you want the project to accomplish. For example: Having your staff dependent on Excel spreadsheets to share and update donor information can be time consuming, and it increases the likelihood of mistakes. Is it time to upgrade to a centralized database that will consolidate donor information in one place, provide access to multiple people, generate meaningful reports, and reduce duplication of effort and data?

Step 2: Write a request for proposal (RFP)

A request for proposal is a document sent to potential consultants so they can:

- Quickly understand the nature of your project
- Know who to contact and when to contact them
- Have guidelines to use when drafting their proposal

An RFP should outline the terms of engagement and clearly state your needs and the criteria you will use when selecting a consultant. Make sure to include:

1. Your organizations mission or goals for the project
2. Background of your organization
3. The problem or need
4. The anticipated outcome
5. What the consultants should include in their proposal bid
6. The criteria you will use to select candidates
7. The deadline for proposal submissions

Be careful not to make the proposal process too complex or time consuming for respondents. The purpose of this step is to act as a screen for disinterested, unprofessional, or unqualified consultants. It should not scare away busy, yet otherwise qualified, firms.

To view sample RFPs, visit:

Step 3: Research

Recommendations are often the best way to find a skilled consultant. Inquiring at agencies similar to your own, you will be able to quickly assess the competencies and professional behavior of consultants they have worked with in the past. This saves you...
the headache of having a carefully screened and researched candidate turn out to be unreliable.

If word-of-mouth doesn’t produce any prospects, search the internet for firms in your area. Many state associations maintain lists of consultancies with contact information on their websites.

Technology is a very broad subject and there are many different types of consultancies. Before you begin compiling a list of RFP recipients, make sure that the company’s realm of expertise fits the nature of your project. It would be a waste of time to send your web development proposal to a company that specializes in telecommunications.

Most IT consultants will have a website and that will be a great place to gather information. Portfolios showcasing past projects are common. You can even find case studies detailing how a firm approached, and ultimately solved, a problem. Having such information readily available will help you determine if the consultant is a good fit for your organization.

**Step 4: Contact candidates**

Once you have written the RFP and researched consultants in your area, it’s time to make contact. The first step is to send your RFP to prospective agencies. It is wise to post RFPs to a public forum such as your website, blogs, social networking sites, or The RFP Database\(^\text{13}\) to ensure that you attract the most qualified prospects, but you should also send your requests directly to consultants that you have researched independently. Make sure to ask for references from everyone you contact.

After you receive enough proposals, you should screen all bids and select a handful of the most promising to interview. Some things you should look for during the interview:

- Familiarity and expertise in relevant areas
- Engaged interest in your organization
- Proven results in similar projects
- Measurable data to show success

Limit the number of candidates you interview to between three and five at one time. If you don’t find a qualified consultant in the first group, contact a few more. By grouping interviews in this fashion, it will help maintain focus and prevent information overload.

Tips and sample interview questions can be found here: [https://www.extension.purdue.edu/extmedia/EC/EC-719.pdf](https://www.extension.purdue.edu/extmedia/EC/EC-719.pdf)

When interviewing and selecting candidates, it is important to ask questions about the project management processes that the consultant organization uses. Ideally, consultants should provide:

- Regular status updates (from once a week to once a month, depending on the size of the project);

---

• Opportunities to ask questions and voice concerns during the process; and
• A dedicated contact at the consultant organization, as well as contact information for a supervisor.

**Step 5: Selection and final documents**

Now that you have put your prospective consultants through an extensive screening and interview process, it is time to make a choice. There is no hard and fast way to decide which consultant to choose. Look at the consultant’s proposal and the notes you made during interviews to try and piece together an understanding of your candidates. Pick whichever firm you feel most comfortable with.

Once you have selected a winning bid, make sure to properly finalize the agreement by drafting:

1. Letter of Agreement (or formal contract)
2. Non-disclosure Agreement

**Letter of Agreement**

For short-term projects, a formal contract should not be necessary. Instead, write up a simple letter of agreement, making sure to include the following items:

1. Services that are to be provided by consultant
2. When interim reports will be provided
3. Beginning and ending dates of project
4. Comprehensive list of fees and necessary materials

For long-term projects, it is advisable to hire legal help to draft a formal contract or review the contract provide by the consultant.

A sample letter of agreement is available here:  

**Non-disclosure Agreement**

To protect your business interests and reputation, you will want your consultants to sign a non-disclosure agreement. This will insure that any sensitive internal information will remain within your organization.

A sample nondisclosure agreement is found here:  

Attachment I

Information Technology

Data Security and Integrity

With the digitization of business processes, organizations are collecting and storing more data than ever before. All data should be secure and backed-up. Data protection should be a top priority for all data including mission-critical and sensitive information from donors and partners. There is an implicit understanding that if supporters trust you with their personal data, you are going to do everything in your power to keep that data safe. Below are a few methods to improve your data security processes.

Regular Backups
Imagine what would happen if you lost your e-mail lists, your donor lists, or your contacts list. How long would it take to recover that information? Would it even be possible? Many nonprofits have been forced to close their doors due to data loss of this type. Make sure it doesn’t happen to you by creating the following:

Backup Schedule
Some organizations backup their systems at the end of each day. For smaller operations, this may not be necessary. Instead, analyze your workflow and identify periods of high-volume file creation or manipulation, and schedule backup times to coincide with those periods. This will ensure that you are not investing time to backup a system that has not undergone significant change. In addition, your organization should routinely back up important information that is stored on laptops and on computers that are not on the server (e.g., the personal computers of telecommuters.)

Redundancy
For backup to be done correctly there needs to be redundancy in the system. Always create at least two copies of your files. If one copy fails, gets lost, destroyed, or corrupted, you will have another copy intact.

Off-site Storage
A backup is no use in the event of an office disaster or an onsite break-in if it is stored next to the parent system. In the event of an unforeseen catastrophe, having a copy of your files stored in a safety deposit box, at another location, or in the cloud, can be a life-saver.

Test Restores
Organizations should perform a monthly test restore of files to ensure that the backup system is working. If you use a third-party organization to provide backups, contact the organization monthly to ask that they restore several different files. You should restore test restores of donor, e-mail, and other databases every three to six months, as they are more difficult to restore and the process is not generally cost effective for nonprofit organizations to perform more frequently.
Data Security
Contrary to popular belief, hackers are not an organization’s worst enemy in relation to data security. Rather it is the organization itself. Easy to overlook loopholes in business processes can sometimes have serious consequences. To minimize risk, do the following:

- Use a data wiping program when computers are disposed of or donated
- Do not collect unnecessary data
- Encrypt sensitive digital information
- Do not print sensitive information
- Protect data by applying “The Principle of Least Privilege” which states that a user should be given only those privileges needed for him/her to complete the task.

Identity Theft: “Red Flags Rule for Nonprofits”
On June 1, 2010, the Red Flags Rule, established by the Federal Trade Commission (FTC), went into effect. This law, developed in accordance with the Fair and Accurate Credit Transactions Act of 2003, requires businesses and privately run groups, including nonprofit organizations, to design an Identity Theft Prevention Program. The purpose of enacting this rule is to decrease the occurrence of identity theft by encouraging employers and employees to be attentive to “red flags” within their workplace that may indicate identity theft. The Red Flags Rule arose out of concern over increasing rates of identity theft and prior, inadequate government regulations. It is hoped that the new rule will “close the loop on identity theft by making it harder for criminals to use stolen identities” as stated in an article by Grant Thornton Advisory Services.

Whether an organization or business needs to adhere to the Red Flags Rule is determined by the activities the group conducts and if these activities are listed by the FTC as vulnerable to fraudulent behavior. Under the Red Flags Rule, some nonprofit organizations participate in activities that could potentially warrant problems with fraud. The rule applies to those nonprofit organizations “that regularly defer payment for goods and services or provide goods and services and bill the customer later,” also referred to as “creditors” by the FTC.

To assist organizations in creating their Identity Theft Prevention Program several resources have been made available by the FTC and other groups concerned with identity protection. A valuable resource provided by the FTC is a compliance template, which allows an organization to assess their level of risk for identity theft and includes a second section that outlines the four-step process necessary to establish a program:

1. Identifying relevant red flags
2. Detecting red flags
3. Responding to red flags
4. Administering your program

In addition to the compliance template, other resources include articles stating the importance of having a program and sample programs.

For a well-designed sample program, see the Identity Theft Prevention Program developed by the Association of County Commissions of Alabama (ACCA). In detail, the ACCA program states the administration of the program, the different types of possible red flags, the need for
covered accounts, and steps to identity theft prevention. Although an organization’s plan should be tailored to their individual characteristics, this document serves as a basic, general outline. The sample program can be found at the ACCA link listed below.

**Risk Analysis, Business Continuity, and Disaster Recovery**

How would your organization respond if your server crashed? If there were a power outage? If several staff became sick? If you were suddenly unable to operate from your physical building? Organizations should perform an analysis that seeks to understand the types of disasters that might affect an organization and begin thinking about how their systems and services would be affected.

Your organization should develop a plan to ensure that you are able to provide key services during a disaster, and that you are able to restore services as quickly as possible. Organizations must assess what levels of resources they are willing to invest in to ensure business continuity and quick disaster recovery. (The Nonprofit Coordinating Committee of New York provides a comprehensive planning document that can help guide you through the process of developing business continuity and disaster recovery plans: [https://www.npccny.org/disaster-plan/](https://www.npccny.org/disaster-plan/)

**Additional Resources**


ACCA: “Sample Identity Theft Prevention Program”

Attachment J
Information Technology

Getting Started with IT Planning

Step 1: Leadership/Management
A few simple questions need to be answered before you start with IT planning.
1. Who in management manages and leads the overall IT for your organization?
2. Who makes the final decisions regarding IT issues for your organization?

Establishing a team or committee to guide the planning process can help to build buy-in among employees and can be an opportunity to incorporate diverse perspectives on IT needs and opportunities. Expectations for team participation responsibilities should be defined and communicated to participants at the beginning of the process.

Step 2: Take a technology inventory and perform a self-assessment
Each organization has unique needs and capabilities. The first step should therefore be to find your starting point.

A technology inventory will allow you to see exactly what hardware, software, and virtual systems you should work with and identify areas where the infrastructure needs strengthening.

A self-assessment requires you to answer several questions about your organization. You will use these questions to make your processes and procedures more effective. For organization-wide results, you can use an online survey service such as Survey Monkey\textsuperscript{14} to collect qualitative information on technology needs from staff and other stakeholders.

Some questions you can ask during a self-assessment:
1. Is the technology inventory current? How many computers do you own? How many servers? Which software packages and operating systems have you installed? Do you have enough software licenses? What technology skills does your staff possess? How much do they know about different hardware and software topics?
2. Do you have any written policies relating to the use of technology in your organization? Do you have any informal, unwritten policies that need to be documented?
3. What are your procedures and policies regarding data backup, computer security, technology purchasing, change requests, tech support, etc.?
4. What is the current state of your website, your local network, your Internet connection, and other key technologies? Are there any weaknesses or threats that need to be addressed?
5. Who do you turn to for advice about information technology?
6. What are the roles and responsibilities in your organization that relate to technology? Are these documented?

\textsuperscript{14}Survey Monkey, http://www.surveymonkey.com
7. Who are your technology vendors and sales representatives?
8. Who provides your Internet connection? How fast is that connection? What sorts of networking equipment (routers, switches, firewalls) do you have?
9. What are the major technology services you provide to your staff, volunteers, donors, and other stakeholders?
10. Do you provide training opportunities for your staff, volunteers, and others who use your technology resources?
11. Are you currently working on any new technology projects or services?

(Questions gathered from Techsoup.org\textsuperscript{15})

There are many free, open-source (free and non-proprietary) technologies that are incredibly helpful for taking a technology inventory and self-assessment. Programs like TechAtlas, Belarc Advisor, or DameWare will automatically identify all hardware and software installed on your computer. It also provides a self-assessment survey that can instantly recommend plans for improvement based on your answers. If you would rather do things by hand, Techsoup.org maintains ready-made forms to help simplify the process.\textsuperscript{16}

Finally, you should assess the relative priorities of the planned projects in terms of potential of benefits and complexity of implementation. For example:
- “Big Wins” can be characterized as projects high potential and high complexity
- “Quick Hits” are high-potential, low-complexity projects
- “Leave for Nows” are low-potential, high-complexity
- “Nice to Haves” are low-potential, low-complexity projects

\textit{Step 3: Design plans for improvement}

In this step, the information gathered from the inventory and self-assessment is analyzed and used to construct a plan that will improve your organization’s technological health. Is your staff undertrained? Do you have programs that you cannot find licenses for? These are problems that must be addressed. A multidisciplinary team should be part of the solution-creation phase. This is the critical part of the planning process. It requires participation of at least one individual with knowledge of available technological tools and processes.

Questions that need to be considered include:
- What software is needed?
- What hardware will that software need?
- Do we need an internal or external network?
- What licenses are required?
- What maintenance is needed (is there a service agreement)?

\textsuperscript{16}“Are your Technology Priorities in Order? Take the Tech Self-Assessment,” Techsoup Canada, \url{https://www.techsoupcanada.ca/en/community/blog/are-your-technology-priorities-in-order-take-the-tech-self-assessment}
• Will we have to upgrade? How often?
• Can the system expand or grow?
• Is it compatible with other solutions we have in place?
• Is there a transition/migration cost?
• How much time will it take to implement?
• How much time is needed to administer and maintain the system?
• What training is needed to use the system?
• What redundancy/security is in place to protect the technology and the data?
• Will the new system force changes/upgrades to other systems?

It is very important that solutions be based on a robust needs assessment. Many vendors, programmers, and software developers will claim that they have the “best” system or that they can make it do this or that. Remember, you are looking for the best solution to your specific needs. A solution that seems too good to be true, often is. A good solution can clearly be mapped onto the organization's needs in a clear and understandable way.

Take special note of the following:

1. Do not attempt to move forward without guidance from an IT professional. Guidance can come from an internal IT expert or an external consultant, but a firm grasp of technology is essential in locating the most useful tools.
2. Do not allow IT personnel to tackle problems alone. If you are lucky enough to have an internal IT expert, do not be tempted to let that person be the sole individual creating a solution for the organization. It is important that all departments and operations are represented in the planning phase.

However, your organization decides to proceed, remember not to overextend your reach. This process is designed to help you identify and eliminate weaknesses in your technological core, not to provide unrealistic goals for solving every technology issue or organizational challenge.

Step 4: Implementation
Once reasonable solutions are conceived, a strategy to implement those solutions must be created. Your strategy should outline:

1. Step-by-step breakdown of the individual tasks required to complete the project
2. Timeline and milestones for each task to allow for measurable progress
3. The resources to be used (equipment, staffing, etc.)
4. The participating staff and the tasks to which they are assigned
5. All projected costs including overhead

It is at this point that hiring a quality specialized consultant becomes necessary for some organizations. A good consultant (or internal employee serving as the project manager) will make sure that the efforts are organized and on schedule and will be able to give honest, accurate feedback, but a poor consultant can single-handedly unravel a well-laid plan.
Attachment K
Information Technology

Sample
Nonprofit Style Guide

This Guide generally follows the Associated Press Stylebook for style preferences.

Every board member and staff person should have a copy of the organization’s style guide, or be able to access a copy easily. The Guide should be included in all employee orientation/training processes and each stakeholder should be held accountable for adhering to it.

Table of Contents

A
Abbreviations
Acronyms
Active voice
Addresses
“And”
Apostrophes
B
Board
Board chair
Board member
Boardroom
Bylaw
C
Capacity building
Citations
Colors
Co-branding
Committee
Corporate form
Courtesy titles
Credentials
D
Dash
Data
Dates
Disabilities
Dollar and other numeric amounts
E
Electronic media
F
First
For-profit
Font
Footnotes (added; incomplete)
Foundation
Fundraising
Fundraiser
G
Grammar Notes
Grantmaking
Grantmaker
Grassroots
H
Hyphenation
I
In-kind
Inc.
Internet terminology
L
Less vs. fewer
Logo
Long sentences
Low-income
M
Media
Memos
N
Nonprofit
Numbers
O
Ongoing
Organization
P
Paragraph spacing
Percentages
Policymaking
Power Point Presentations
Programs
Punctuation
Q
Quotation marks
R
Racial Language
“Really”
S
Semi-colons
Sexuality (language in reference to)
Start-up
States
T
That vs. which
Time
Titles
“Very” Volunteerism web-based work plan Year-round
**Abbreviations**

- Don’t use postal abbreviations (MD, VA) in text **except** when referring to multiple locations in write-ups. (see STATES)
- NE, NW, SE, SW
- Spell out United States

**Acronyms** – Spell out organization names on first reference. Use acronyms later. As a rule, only use acronyms if they are well known; don’t make them up. For example, “Internal Revenue Service” – spell out full name (capitalized) on first reference, and “IRS” is acceptable on second reference.

**Active voice** is always better than passive voice (Anytime it is not clear from a sentence who is doing the action, it is probably passive.). **Passive:** A decision was reached that you should be fired. **Active:** I decided to fire you.

**Address format** – Describe how your organization’s address should be formatted.

“**And**” should be spelled out. The ampersand ‘&’ should only be used if it is officially part of a proper name or organization

**Apostrophes:** Watch this in particular with references to organization names.

**Board** is singular and is not capitalized. **Board members** is plural, two words, and not capitalized. *The board is meeting in the conference room. The board is excited about its new strategic plan.* OR *The board members are ready to meet. They have worked hard on this strategic plan.*

**Board chair** is preferable to chairman, chairwoman, or chairperson.

**Board member** is the preferred generic terminology, as opposed to trustee or director. At many foundations, however, trustee is used. Go with the preference of the organization you’re referring to.

**Boardroom** is one word.

**Bylaw** is one word, no hyphen.

**Capacity building** is two words when used as a noun (e.g. *Organization is engaging in capacity building*). However, it is hyphenated when used as an adjective (e.g., *Organization has a new and exciting capacity-building strategy*).
Citations – see Turabian, Kate, *A Manual for Writers of Term Papers, Theses, and Dissertations 6th ed.* 1996.

Colors – Insert information about color palettes in place for your organization

Co-branding: On all program documents – be sure that “Project of [Organization]” is stated prominently with the organization’s logo.

Committee should be treated like the word board, and not capitalized. (e.g. “We’re inviting the investment committee to meet on Thursday.”)

Corporate form – use LLP not L.L.P.

Courtesy titles – Refer to both men and women by first and last name: Jill Jones or Mike Jones. Use the courtesy titles Mr., Miss, Ms., or Mrs. only in direct quotations or when specifically requested. See Titles.

Credentials – use CPA not C.P.A and CFRE not C.F.R.E.

Dash – there are differences between hyphens, en dashes, and em dashes.

- Hyphens are used within words, as in “write-ups” (use hyphen/dash key)
- En dashes are used like the word “to,” as in “ages 3 – 5”
- Em dashes are used to separate out a phrase for emphasis or dramatic effect. (e.g. “The fundraiser was so successful — bringing in $5 million — that we decided to do another one next year.”)

Data is plural. Make sure your verbs and possessive pronouns agree in number. (e.g. *The data are stored in the research folder.*)

Dates – write numbers using only numerals (cardinal number) rather than 1st, 2nd, 3rd, 21st (ordinal number) (e.g. “The fiscal year starts July 1.”) Using ordinal numbers is more common and acceptable in speech or conversational writing (e.g. “We had a delightful picnic on the 4th of July.”) Use date format: September 20, 20xx. Do not use “September 20th”. If you do not use the numeric day in the date, it should read ‘September 20xx’ not ‘September, 20xx’ (no comma required).
Put people first, not their disability
Comment: Preferred expressions avoid the implication that the person as a whole is disabled or defective.

**PREFERRED**
- person with (who has) a disability
- child with a congenital disability
- child with a birth impairment
- person with mental illness or psychiatric disability

**PROBLEMATIC**
- disabled person
- birth defective child
- birth impaired child
- mentally ill person

Dollar and other numeric amounts – when exact amounts are not critical to report, it is generally preferable to use rounded amounts. In general, do not use cents for dollar amounts over $99.99 or a decimal for amounts in the three digit millions or billions: “the $700 billion rescue package,” “the state has a $243 million projected shortfall this fiscal year,” “the special session of the legislature approved $1.3 billion in additional revenues.”

Electronic media – Below is a list of common terms and their preferred spelling.
- database
- e-mail
- FTP
- Internet
- LISTSERV* (tm) – the generic term is electronic mailing list
- online
- PDF
- URL
- Web

First – not 1st for numerical order.

For-profit is hyphenated.

Font for external documents: Insert fonts that have been chosen for the organization. For headers, use xxx; for normal text, use xxx or xxx. Font size should be at least 11 pt. Organization’s e-mails and website should use xxx.

Footnotes: Do not use footnotes to reference information. Use an in-text citation such as, "According to the Standards for Excellence codes, “Communications, Engaging the Public and Social Media” bulletin…” Do not use footnotes to add anecdotes or extra information to your article.
Use the same method of citation regardless of your source. Books and journal articles, for example, should both be cited in the same method.

**Foundation** is capitalized on second reference when referring to a specific foundation (not foundations in general).

**Fundraising, fundraiser** is one word.

**Grammar Notes** – Avoid use of contractions (e.g. It IS in the conference room; versus It’s in the conference room). Reflexive pronouns – when referring to people use “who,” when referring to organizations, use “that”.

**Grantmaking, grantmaker** is one word.

**Grassroots** is one word.

**Hyphenation**– Hyphenate words like decision making and conflict of interest only when used to modify a noun. Do not hyphenate these words when used as nouns. Examples: *Improve your decision-making skills. Let young people get involved in organizational decision making. I suspect there is a conflict of interest there. Every board should have some sort of conflict-of-interest policy.* (except policymaking, which is one word)

**In-kind** is hyphenated when it is used as an adjective, as in “in-kind donation”

**Inc.** should not be used unless it is part of the organization’s name that it uses every time it mentions its name. Please do not put Inc. in an organization’s database record. If Inc. must be used, set it off with a comma. If it is in the official name, use it on first reference, and drop it for subsequent references.

**Internet terminology**
- **Internet, World Wide Web:** proper nouns, capitalize
- **website:** one word, no hyphen
- **web page:** two words, no hyphen
- **e-mail:** hyphenated, lowercase
- **online:** one word, no hyphen
**Less vs. fewer** – Less should be used with nouns that *can’t* be counted, as in “let’s talk in here where there is less noise.” Fewer should be used with nouns that *can* be counted, as in “fewer people showed up for the rally than we expected.”

**Logo** – The organization has one logo – describe logo. The logo can be found [INSERT LOCATION].

**Logo Guidelines**
- Never change the colors of any part or parts of the logo
- Never skew, tilt, copy, paste, enlarge, or shrink the logo
- Never change the size of the logo beyond the minimum size. Writing should ALWAYS be readable.
- Never add additional elements to the logo
- Never rearrange the elements of the logo
- Never print the logo over a patterned background or place it on a background that would compromise the readability of the elements
- Never crop the logo or let it bleed off the page
- Never change the proportional sizing of the logos

**Logo Color Options**
The logo should only appear in the designed colors. There is also a black and white option. Select the color scheme that will create the most contrast with the background and does not clash with other colors.

**Clear Space**
Assure that there is ample white space around the logo so it does not appear crowded.

**Sizing standards for organization logo:**
- Big Logo: (H)1.48” by (W)3.5”
- Medium Logo: 1.06” by 2.5”
- Minimum Size: 0.64” by 1.5”

**Long sentences** containing many clauses, commas, semicolons, and that run-on to several lines should be shortened. If a sentence contains a long list of items, particularly complicated items, separate them out into a bulleted list.

**Low-income** is hyphenated when used as an adjective. If low and moderate are both descriptions of kind of income, they both require hyphens, even if separated from income. (e.g. “Kathy’s 24-hour clinic serves children from low- and moderate-income families.”)

**Media** is plural. Make sure your verbs and possessive pronouns agree in number.
**Memos** are only used for internal purposes. When writing a Memo, the logo should still be in the header and the standard format is:

Memorandum  
Date  
To:  
From:  
CC:  
RE:  

**N**  

**Nonprofit** – One word, **no hyphen**.

**Numbers** (see also dollar and other numeric amounts above)

- Numbers 10 and above are written in numerals, nine and under should be spelled out.  
  *Exception* – if a sentence contains numbers like nine and 103, you should default to the numerals, and make them 9 and 103.
- Decades should be written as 1930s not 30s or ’30s.
- Use hyphens between numbers of rulings, *a five-to-four ruling*.
- Format phone numbers using periods as in the letterhead, 202.452.6262.
- When writing toll-free or long distance numbers, do not list the “1-” before the 10-digit number.
- When writing percentages, use the numeral for all values and *spell out percent*. 4 percent. Use % when in a table or figure.
- When writing monetary values, always use the dollar sign and the numeral for values under 1 million. Spell out million or billion and round down the nearest tenth. Never spell out dollars except in general use. *I found a dollar. I have $1.50. He won $4.2 million in the lottery.* Use dollars and cents, even if there are no cents (i.e. $50.00).
- Write times as follows: *11 am, 5 this morning, at 10:30 last night,* Do not write 11:00 or 11 o’clock. **Make sure am and pm are always lowercase without periods and a single space between the time and the am or pm reference.** Be sure not to be redundant in writing time. *I woke up at 7 am in the morning.*

**O**  

**Ongoing** is one word.

**Organization** is singular. Make sure your verbs and possessive pronouns agree in number. *The organization has 10,000 members.*
Organizational Name: XXX is our legal name. We commonly use our trade name, xxx, not yyy or YYY. However, when using our trade name within a document, you should spell out our entire trade name for its initial use, and you may refer to us as xxx afterwards.

P

Paragraph spacing – either indent or insert an extra line of space to distinguish a new paragraph. Do not do both.

Percentages – spell out the word percent (e.g. “next year only 20 percent of our budget will come from foundations.”) Also see Numbers.

Policymaking – is one word.

Powerpoint Presentations for Organization can be found here XXXX.

Programs – Organizational programs and services should be listed in alphabetical order as follows:

(Insert official program titles here)

Punctuation

• Use commas before “and” and “or” at the end of a series. We bought apples, oranges, and bananas.
• Use a comma between the name and a suffix. Sammy Davis, Jr.
• Do not use slash “/” in text unless part of a name.
• Place one space before — and after — em dashes.
• Dashes and hyphens – see Dash
• Put one space between sentences, not two.

Q

Quotation marks – Double quotation marks are used in the following ways:

• around directly quoted material
• song titles
• short-story titles
• short-poem titles
• articles appearing in any periodical (newspaper, magazine, journal, newsletter)
• essays
• episodes of television or radio series
• chapter titles of books
• around words being used in a special, abnormal sense — do not put quotes around slang words or phrases
R

Racial Inclusive Language – racial/ethnic groups are designated by proper nouns and are capitalized. When names of colors are used to refer to human groups, they are capitalized (e.g., Blacks instead of blacks; Whites instead of whites). Hyphens are not used in multiword labels (e.g., Mexican Americans instead of Mexican-Americans).

Really: Don’t use the word “really” it undermines the effectiveness of the word that you’re modifying. Make your point without it, or choose a new word as your subject.

S

Semi-colons – are generally used for two reasons. According to AP “use the semicolon to indicate a greater separation of thought and information than a comma can convey but less than the separation that a period implies.”

1. Clarify a series
   Use semicolons to separate elements of a series when individual segments contain material that also must be set off by commas.

   e.g. The menu for the day included, for brunch, quiche, cantaloupe, and croissants; for tea, chamomile and crumpets; and for dinner, roast beef, potatoes, and asparagus.

   The point of using a semicolon here is to avoid confusion that might occur if the wrong items are attached to particular lists.

2. Linking independent clauses
   If two clauses are not joined by a conjunction (and, but, or, yet, for, nor, so) and form a compound sentence, use a semicolon to connect them.

   e.g. The taxi refused to take me to 50th Street; I had to catch a ride with Kathy.

   So if you don’t like using the semicolon in this way, your options are to add a conjunction, or split the sentence into two.


Start-up is hyphenated, as in “She’s the head of a successful Internet start-up” or “We often fund start-ups if their board leadership is strong.”

States – primarily for the purpose of text, where space is at a premium and there are often multiple locations listed for a nonprofit’s service area, use Montgomery County (MD), Falls Church (VA), Prince George’s County (MD), rather than spelling out the state name. (e.g. the Institute serves families in Montgomery County (MD) and Washington, DC.)
That vs. which

- Use **that** to introduce a clause that contains information essential to the meaning of the sentence. Do not use a comma before “that.” *The Nile is the river that gives Egypt life.*
- Use **which** to introduce a clause containing information that is not essential to the meaning of the sentence. Set off the nonessential clause with commas. *The Nile, which flows into the Mediterranean, gives Egypt life.*

**Time** – use am and pm without periods. *(see Numbers)*

**Titles** are always capitalized.

**Very** – don’t use the word “very” it undermines the effectiveness of the word that you’re modifying. Make your point without it or choose a new word as your subject.

**Volunteerism** – rather than voluntarism

**Web-based** has a lowercase w and is hyphenated when used as an adjective.

**Work plan** is two words.

**Year-round** – hyphenated when used as an adjective

Insert a list of the organization’s registered trademarks if any.
Sample Communications Policy

Purpose:
1. To ensure consistent projection of the most positive, professional, and accurate organizational image to the public.
2. To facilitate effective, professional, and respectful communications between and among the board, organizational management, and the staff.

Public Relations and Policy Communications / Relations
The chief executive should be informed of all media inquiries and given the opportunity to respond or delegate to the appropriate staff member. In the absence of the chief executive, the (insert position titles) are authorized spokes-people. At all times, responses will adhere to (THE NONPROFIT)’s mission, strategic goals, and public policy principles. When an inquiry falls outside of our expertise, we will make a referral to an appropriate expert.

Internal Communications
All internal communications - written and oral - will be professional and respectful in nature and free from any inflammatory or profane language. The staff email and intranet are to be used for professional communications only. Wherever possible, internal emails should be minimized in favor of communicating via the intranet.

The chief executive must authorize professional communications with board members unless they involve communications per our personnel and whistleblower policies. The chief executive may directly delegate to staff members any regular communications with board members around committee work, etc. Email communications between staff and board members should be CC’d to the chief executive.

Trademarks, Logos, and Seals
(THE NONPROFIT) shall maintain a style guide that governs all logos. (THE NONPROFIT) logo and name shall be trademarked.

External Communications
All communications on (THE NONPROFIT) letterhead or email masthead template should be approved by director-level staff. All external communications should be proofread by someone other than the original author.

Our communications will be compliant with all relevant equal opportunity and other legal requirements.

- **Equal Employment Policy Statement**: The Employee Handbook should include an Equal Employment Opportunity statement.
• **Copyright Statements**
• **Maryland Charitable Solicitations Act Requirements:** All written solicitations materials and receipts must contain the following disclosure statement, “Maryland Nonprofits is a U.S. tax-exempt 501 (c)(3) organization, donations to which are tax deductible to the fullest extent allowed by law. Consistent with IRS guidelines, Maryland Nonprofits affirms that no goods or services were provided to you in exchange for your donation. A copy of our current financial statement is available upon request by calling our office. Documents submitted to the State of Maryland under the Maryland Charitable Solicitations Act are available from the Secretary of State, State House, Annapolis, MD 21401 for the cost of copying and mailing.”
  - See also *(THE NONPROFIT)* Handbook

**Brand Management**
When individuals or organizations are given permission to utilize *(THE NONPROFIT)* brand, logos, and/or name, care should be taken to ensure that proper permissions are described in writing, such as in licensing or marketing agreements or other documentation as appropriate. Permission to utilize *(THE NONPROFIT)* brand, logos, and/or name should be given with the approval of the CHIEF EXECUTIVE and/or his/her designee.

**Privacy, Security & Confidentiality**
(Refer to Technology Policy)

**Crisis & Disaster Planning and Communications**
(Refer to Emergency Action Plan)

**Communications Plan**
The chief executive is responsible for developing a communications plan to articulate and implement this policy for the organization.

Attachment M
Communications and Social Media

Sample
Social Networking Policy

Source: The Arc Baltimore, reprinted with permission, 2014

The Arc Baltimore takes no position on your decision to start or maintain a blog or participate in other social networking activities. However, it is the right and duty of the company to protect itself from unauthorized disclosure of information. The Arc Baltimore’s social networking policy includes rules and guidelines for company-authorized social networking and personal social networking and applies to all staff.

General Provisions
Blogging or other forms of social media or technology include, but are not limited to, video or wiki postings, sites such as Facebook and Twitter, chat rooms, personal blogs or other similar forms of online journals, diaries, or personal newsletters not affiliated with The Arc Baltimore. Unless specifically instructed, employees are not authorized and therefore restricted from speaking on behalf of The Arc Baltimore. Employees may not publicly discuss clients, products, employees, or any work-related matters, whether confidential or not, outside company-authorized communications. Employees are expected to protect the privacy of The Arc Baltimore and its employees and clients and are prohibited from disclosing personal employee and nonemployee information and any other proprietary and nonpublic information to which employees have access. Such information includes, but is not limited to, customer information, trade secrets, financial information, and strategic business plans.

Employer Monitoring
Employees are cautioned that they should have no expectation of privacy while using the internet. Your postings can be reviewed by anyone, including The Arc Baltimore. The Arc Baltimore reserves the right to monitor comments or discussions about the agency, its employees, clients, and the industry, including products and competitors, posted on the internet by anyone, including employees and non-employees. The Arc Baltimore uses blog-search tools and software to monitor forums such as blogs and other types of personal journals, diaries, personal and business discussion forums, and social networking sites.

Employees are cautioned that they should have no expectation of privacy while using company equipment or facilities for any purpose, including authorized blogging.

The Arc Baltimore reserves the right to use content management tools to monitor, review, or block content on company blogs that violate company blogging rules and guidelines.

Reporting Violations
The Arc Baltimore requests and strongly urges employees to report any violations or possible or perceived violations to supervisors, managers, or the HR department. Violations include
discussions of The Arc Baltimore and its employees and clients, any discussion of proprietary information, and any unlawful activity related to blogging or social networking.

**Discipline for Violations**
The Arc Baltimore investigates and responds to *all* reports of violations of the social networking policy and other related policies. Violation of the agency’s social networking policy will result in disciplinary action up to and including immediate termination. Discipline or termination will be determined based on the nature and factors of any blog or social networking post. The Arc Baltimore reserves the right to take legal action where necessary against employees who engage in prohibited or unlawful conduct.

**Acknowledgment**
Employees are required to sign a written acknowledgement that they have received, read, understood, and agreed to comply with the company’s social networking policy and any other related policy.

**Authorized Social Networking**
The goal of authorized social networking and blogging is to become a part of the industry conversation and promote web-based sharing of ideas and exchange of information. Authorized social networking and blogging is used to convey information about agency products and services, promote and raise awareness of The Arc Baltimore’s brand, search for potential new markets, communicate with employees and customers to brainstorm, issue or respond to breaking news or publicity, and discuss corporate, business-unit, and department-specific activities and events.

When social networking, blogging, or using other forms of web-based forums, The Arc Baltimore must ensure that use of these communications maintains our brand identity, integrity, and reputation while minimizing actual or potential legal risks, whether used inside or outside the workplace.

**Rules and Guidelines**
The following rules and guidelines apply to social networking and blogging when authorized by the agency and done on company time. The rules and guidelines apply to all employer-related blogs and social networking entries, including agency subsidiaries or affiliates.

Only authorized employees can prepare and modify content for The Arc Baltimore’s blog located on The Arc Baltimore’s homepage, and/or the social networking entries located on sites such as Facebook or Twitter. Content must be relevant, add value, and meet at least one of the specified goals or purposes developed by The Arc Baltimore. If uncertain about any information, material, or conversation, discuss the content with your manager.

Any copyrighted information where written reprint information has not been obtained in advance cannot be posted on The Arc Baltimore’s sites.

Business units and departments are responsible for ensuring all blogging and social networking information complies with The Arc Baltimore’s written policies. Department heads are
authorized to remove any content that does not meet the rules and guidelines of this policy or that may be illegal or offensive. Removal of such content will be done without permission of the blogger or advance warning.

The Arc Baltimore expects all guest bloggers to abide by all rules and guidelines of this policy. The Arc Baltimore reserves the right to remove, without advance notice or permission, all guest bloggers’ content considered inaccurate or offensive. The Arc Baltimore also reserves the right to take legal action against guests who engage in prohibited or unlawful conduct.

**Personal Blogs**
The Arc Baltimore respects the right of employees to write blogs and use social networking sites and does not want to discourage employees from self-publishing and self-expression. Employees are expected to follow the guidelines and policies set forth to provide a clear line between you as the individual and you as the employee.

The Arc Baltimore respects the right of employees to use blogs and social networking sites as a medium of self-expression and public conversation and does not discriminate against employees who use these media for personal interests and affiliations or other lawful purposes.

Bloggers and commenters are personally responsible for their commentary on blogs and social networking sites. Bloggers and commenters can be held personally liable for commentary that is considered defamatory, obscene, proprietary, or libelous by any offended party, not just The Arc Baltimore.

Employees cannot use employer-owned equipment, including computers, company-licensed software, or other electronic equipment, nor facilities or agency time, to conduct personal blogging or social networking activities.

Employees cannot use blogs or social networking sites to harass, threaten, discriminate, or disparage against employees or anyone associated with or doing business with The Arc Baltimore.

If you choose to identify yourself as an Arc Baltimore employee, please understand that some readers may view you as a spokesperson for The Arc Baltimore. Because of this possibility, we ask that you state that your views expressed in your blog or social networking area are your own and not those of the company, nor of any person or organization affiliated or doing business with The Arc Baltimore.

Employees cannot post on personal blogs or other sites the name, trademark, or logo of The Arc Baltimore or any business with a connection to The Arc Baltimore. Employees cannot post company-privileged information, including copyrighted information or company-issued documents.

Employees cannot post on personal blogs or social networking sites photographs of other employees, clients, vendors, or suppliers, nor can employees post photographs of persons engaged in company business or at company events.
Employees cannot post on personal blogs and social networking sites any advertisements or photographs of company products, nor sell company products and services. If contacted by the media or press about their post that relates to The Arc Baltimore business, employees are required to speak with the Executive Director, Chief Advancement Officer, or their designee before responding.

If you have any questions relating to this policy, your personal blog or social networking, contact your manager or Human Resources.
Attachment N

Essential Communication Tools
Reprinted with Permission of Author, Sally J. Patterson.

APPENDIX 1

ESSENTIAL COMMUNICATION TOOLS

Organizational description
Often called the “elevator speech” or the “cocktail party description,” this simple, 20- to 25-word description explains what the organization does and whom it serves. Using a mission statement or permitting staff and board members to create individualized descriptions causes confusion and misses a valuable opportunity to create enthusiasm and excitement. All staff and board members should use the standard description all the time, uniformly.

Fact sheet
This is a one-page document that has four key elements: the organization description, a brief history, a summary of programs and services, and appropriate contact information. The fact sheet answers the question, “What can our organization do for you?”

Style manual
A guide to maintaining a positive, professional image in all print and online publications, the style manual addresses the use of the logo, typography, color, editorial style, and other factors to encourage consistency in organizational materials (internal and external).

Human interest stories
Helping the public connect to an organization requires telling its story in a way that personalizes the issue and its true impact. However, organizations must be sensitive to their moral and ethical commitments when asking people to “go public” with their stories.

Annual report
Many nonprofit organizations spend much of the communication budget on the annual report, which provides an opportunity to document significant accomplishments, highlight supporters and clients, and present financial information. Annual reports support relations with donors, so they are an excellent vehicle for explaining where the money went and what was accomplished.
Press kit
This standard set of materials is used for all press events. Among the items that should be included are:

- organization fact sheet
- one-page profile of spokespersons (offer to provide photographs upon request)
- issue briefs
- contact list
- press clippings
- optional items, such as the annual report, a copy of the latest newsletter, or a list of coalition partners

IRS Form 990, Return of Organization Exempt from Income Tax
The Form 990 is a public document that reports (among other things) annual revenue and expenses; expense details by program services, management, and fundraising activities related to the organization's exempt purpose; a statement of financial position; and a list of officers and directors, including compensation paid to them. Schedule A lists the five highest-paid employees, the five highest-paid persons for professional services, and details of revenues and expenses. The Form 990 is an opportunity to educate the public about unusual financial circumstances, to highlight organizational milestones and declare future goals, to document revenue streams, and to address management decisions, such as executive compensation and the board's commitment to its fiduciary responsibility.

Web site
Online communication is proactive, interactive, and ongoing. More than just establishing a Web site, it involves finding and posting relevant information, identifying and connecting with current and potential audiences, and possibly developing an online community. A well-organized, well-written, well-maintained, and graphically compelling Web presence is one of the best ways to educate and influence key constituencies. Web sites tend to develop in three phases: information provision; information provision with limited membership feedback (sign-up, order materials, etc.); and a fully integrated site that allows the visitor to interact with the host site.

Social media
Social media use Web-based technologies to transform an organization's one-way communication into a two-way dialogue with key audiences. Social media can take many different forms including Internet forums, CIO blogs, microblogging, wikis, podcasts, pictures, videos, and more. Individual board members can include information on their personal Facebook pages and forward tweets and other updates using their individual Twitter accounts.
Endorsements
Some nonprofits expand their identities by creating a seal of approval around mission-related products or issues. In addition to the Form 990, Independent Sector, GoldStar, and other sites provide membership rosters that give added stature to nonprofit organizations through their own screening and review processes. Others have awards programs honoring those who contribute to advancing their mission or who provide exemplary leadership.