Nonprofit Risk Management Plan

This SAMPLE Risk Management Plan was drafted based on recommendations shared in a board retreat for a real nonprofit. The plan was drafted with the help of a software tool called: "My Risk Management Plan" that is available from the Nonprofit Risk Management Center.

For further information, please visit: www.myriskmanagementplan.org.

Risk Management Plan for NONPROFIT

Risk Management Philosophy
NONPROFIT aspires to operate in a way that protects the health, safety and security of clients, staff members and volunteers while lifting up the organization's mission and safeguarding assets needed for mission-critical programs and activities.

Risk Management Goals
The safety of personnel receiving or engaged in delivering services sponsored by NONPROFIT shall at all times be regarded as a top priority and this emphasis shall be communicated throughout the organization in order to ensure its understanding.

General Safety Principles
The safety of personnel receiving or engaged in delivering services sponsored by NONPROFIT shall at all times be regarded as a top priority and this emphasis shall be communicated throughout the organization in order to ensure its understanding.

NONPROFIT seeks to involve appropriate personnel, whether board or staff, at all levels of the organization in the identification of risks and creation of practical strategies in order to make certain that the organization's approach to risk management considers diverse perspectives and that staff understand their responsibility to protect the confidentiality of our clients, the safety and security of our facilities, the integrity our reputation, the preservation and future growth of assets as well as the fulfillment of our mission.

Responsibility for Risk Management

Board of Directors

- Sets risk management goals, adopts annual operating objectives and budget with risk management included.
- Adopts annual capital budget with risk management in mind.
- Reviews operational reports to determine compliance and future priorities.
- Ensures compliance with policies and standards imposed by national organization or accrediting organization.
- Adopts and establishes policies and standards.
- Reviews the organization's insurance program periodically.
- Reviews the organization's risk management plan annually.

Executive Director or CEO

- Assigns staff to design and carry out safety and risk management activities.
- Assigns staff to perform annual review of the safety and risk management activities.
- Executes contracts for the organization.
- Keeps the board apprised of emerging threats and opportunities facing the organization.

[Need to identify additional staff positions that will have responsibility and accountability for various risk management goals.]

Risk Management Committee

- Champions organization-wide effort to protect the vital assets of NONPROFIT and engage key stakeholders in risk management activities.
- Convenes periodically to review the agency's priority risks and corresponding risk management strategies.
- Oversees the development, implementation and monitoring of loss prevention programs.
- Oversees the purchase of insurance for the organization.
- Evaluates the insurance program.

Governance Structure

Articles of Incorporation

NONPROFIT was incorporated in the State/Commonwealth of [state] on [month, day, year]. The articles of incorporation were last reviewed by legal counsel in [month, year] to ensure compliance with state laws. We have maintained our corporate status by filing with the state as required by law. The date of our last filing was [month, day, year]. Board representatives reviewed the articles for compliance with the current mission and purpose of the organization in [month, year]. The Board and legal counsel will review the articles of incorporation every [number] years to maintain its currency and legality.

The original articles of incorporation are stored [storage location name, address] An authenticated copy of the articles are stored [storage location name, address].

Bylaws

The bylaws were originally filed and approved by the State of [state] on [month, day, year]. Board representatives reviewed the bylaws to determine the need for any revisions and if necessary followed the proper amendment process in [month, year]. All amendments were filed with the state and the last filing was made on [month day, year]. The bylaws were reviewed by legal counsel in [month year] to ensure compliance with federal, state and local laws. The Board will review the bylaws annually and propose amendments as needed. Every member of the board receives a current copy of the bylaws when they join the board and whenever the bylaws are amended.

The original bylaws as approved by the state and any amendments are stored [storage location name, address]. An authenticated copy of the bylaws and amendments are stored [storage location name, address].

Indemnification

Legal counsel reviewed the indemnification provision for compliance with state law on [month day, year]. The indemnification provision is funded by a Directors' & Officers' liability insurance policy underwritten by [insurance company] under [policy number] with a term of [policy dates]. The policy limit of liability is [limit] with a deductible of [amount of deductible or retention].

Conflict of Interest Policy
The conflict of interest policy was adopted by the board on [month day, year]. Every year each board member completes and signs a disclosure statement declaring any known conflicts and agreeing to comply with the policy. These annual statements are gathered in [month] of each year.

Board Operations

[Insert here a description of the current status of a board orientation manual or the aspirational goal that NONPROFIT will develop such a manual. Example: "NONPROFIT has adopted a Board Manual containing the key policies and expectations of the board. The Manual is reviewed [every two years] by [the Executive Committee of the board] and updates are made on an as-needed basis.

Board Orientation
To ensure that the members of the Board of NONPROFIT are properly trained and prepared for their service, the organization conducts a board orientation training for all board members on an annual basis. The experienced board members will share their insights and coach the new members in fulfilling their board duties.

Board Development
The board of NONPROFIT is dedicated to improving the skill and knowledge of its members by continually educating the members on the legal, financial, and operational aspects of governing a nonprofit organization. The board will allocate time during the year to increase its governance knowledge.

Board Assessment
To become a more effective board, the board members of NONPROFIT will conduct a board self-assessment at least once every three years. The board will use the self-assessment as a tool to improve its performance and energize the organization to achieve its mission.

Board Recruitment and Nomination
NONPROFIT strives to have a diverse and qualified board with people who bring the skills, qualities, and expertise needed to lead and govern the organization in accomplishing its mission.

Board Minutes
Include here a description of how NONPROFIT maintains important corporate records of board and committee action. Example: " NONPROFIT recognizes the importance of recording accurate and contemporaneous minutes of board meetings and minutes of committees that are authorized to act on the board's behalf, and each board member is aware of his/her responsibility for ensuring the accuracy of the minutes."

"The minutes are maintained [in a safe location] in a separate binder to preserve their integrity."
or
"The minutes are stored with other corporate documents in a safe location to protect them from harm or loss."

[Reference to a document retention plan and its mandate to maintain documents such as the articles of incorporation, IRS Determination letter and board meeting minutes into perpetuity would be appropriate here.]

Risk Financing Strategy

Add appropriate language here that describes the philosophy and accountability for the insurance program at NONPROFIT:

Example: "To safeguard the assets and resources of NONPROFIT, the organization will purchase insurance for those insurable risks of major importance to mission-critical operations and the financial health of the organization. It is the executive director's responsibility to oversee the organization's insurance program and provide an annual insurance report to the board."

Human Resources

Written Employment Policies
NONPROFIT believes that written employment policies are an essential risk management tool. The organization has compiled its key employment policies in a document titled [name of employee handbook or manual].

Communications Regarding Employment Policies
Describe the manner in which employees at NONPROFIT are informed about personnel policies:

Examples:
"All new policies are communicated in writing to staff through the use of memos and other appropriate policy documents. In addition, new policies are incorporated in the policy manual when that manual is updated periodically."
or
"Each time a new employment policy is adopted the employee handbook is re-issued and distributed to staff. Staff members are required to sign an acknowledgement that is maintained in their personnel file, indicating that they received and agree to adhere to the new policy(ies)."
or
"New policies are communicated verbally and in writing to employees. Staff are also required to confirm their understanding of and willingness to abide by any new policies."
Insert here NONPROFIT 's policy concerning the review and updating of your key employment policies.

For example, " NONPROFIT reviews and updates its Employee Handbook every two years in order to ensure that policies remain suitable for the organization and in compliance with state and federal employment laws. The organization obtains assistance from an employment attorney in this effort."

Describe the use of job descriptions by NONPROFIT:

Example: " NONPROFIT has developed job descriptions for all paid [and volunteer] positions in the organization. These documents are finalized before the recruitment process begins and used during interviews with prospective candidates to inquire whether the candidate is able to perform all the duties listed. The positions' essential functions are listed. Each position description for paid staff also includes the classification of the position as either "exempt" or "non-exempt."
or
"NONPROFIT uses job descriptions for both paid and volunteer positions in the organization. These documents are developed by supervisory personnel, reviewed by outside legal counsel, and updated on an as needed basis."

Employee Orientation
Describe here the process used by NONPROFIT to orient new staff/volunteers. Example:

"The Director of Human Resources at NONPROFIT is responsible for conducting a [two-hour] orientation session for all new employees [and volunteers] on the first day of employment. During this session key provisions of the Employee Handbook are discussed, the employee is asked to provide any additional information necessary for benefits enrollment, and the employee is encouraged to ask questions about any aspect of employment policy or operations. Employees are also introduced to other staff and provided with an overview of equipment and systems they will be required to use.
or
"Each supervisor at NONPROFIT is responsible for designing and conducting an appropriate orientation session for their new hires. The orientation must take place within the first week of employment. A typical orientation includes review of key policies, introduction to software programs and hardware programs that will be used by the employee, introduction to other staff and key volunteers, and a review of the supervisor's expectations and reporting requirements."

Staff Supervision
NONPROFIT views effective staff supervision as an essential component of risk management. Supervisory staff are expected to communicate their expectations of direct reports clearly and consistently and hold employees accountable with regard to key tasks and responsibility and compliance with the organization's employment policies. All employees are encouraged to raise concerns or questions about work priorities and assignments with their direct supervisor.

Performance Appraisal Process
Describe your existing strategy or policy concerning Performance Appraisals. Don't forget to include the process for board review of the compensation and performance of the CEO. For example:

NONPROFIT requires annual reviews for all employees. Supervisors are responsible for scheduling review meetings and completing the Performance Review form. A goal-setting exercise is part of this process.

Programs and Services

Counseling and Support Services
To do: With staff who are responsible for this area, note the specific primary risks and risk management strategies NONPROFIT has/will adopt to address the identified risks arising from the Counseling and Support Services function.

Emergency Services
To do: With staff who are responsible for this area, note the specific primary risks and risk management strategies NONPROFIT e has/will adopt to address the identified risks arising from the Emergency Services activities of the organization.
Hotline.

To do: With staff who are responsible for this area, note the specific primary risks and risk management strategies NONPROFIT has/will adopt to address the identified risks arising from Hotline.

Housing Services
To do: With staff who are responsible for this area, note the specific primary risks and risk management strategies NONPROFIT has/will adopt to address the identified risks arising from the Housing program(s).

Education and Training
To do: With staff who are responsible for this area, note the specific primary risks and risk management strategies NONPROFIT has/will adopt to address the identified risks arising from the Education and Training programs of NONPROFIT.

Client Safety

INSERT HERE client safety policies and procedures, and identify who is accountable to ensure they are followed.

If there are policies or practices that NONPROFIT plans to implement in the future, or aspirationally wants to incorporate in the future, identify those and also who will be responsible for their development/implementation and the timeframe for doing so.

Staff Code of Conduct Insert here an existing Code of Conduct for Staff/Volunteers, if you have one, or develop one for this portion of the Risk Management Plan:

Example:
- I understand that my active participation in [Name of Organization]'s program is important to the success of my involvement and the organization's efforts. Therefore I agree to abide by the following rules for my participation.
- I understand that my consistent participation is important and I will honor my time and service commitment.
- I will respect the rights, dignity and worth of all people involved within the program. I will be a positive role model for the clients with which I have contact.
- I understand that the relationship between the clients and me is important and I will not include other people in our activities, including members of the client's or my family.
- I understand that my role as a volunteer (or employee) is a matter of trust and will not pursue any activities with the client(s) outside the confines of the organization's program.
- I understand that I may learn personal information about others that I will keep confidential.
- I will not engage in activities that pose a serious risk of injury to myself and others, including but not limited to, use of alcohol or drugs (illegal or that impair my ability to perform my duties), or smoking in the presence of clients.
- I will refrain from any form of personal abuse towards others, including verbal, physical and emotional abuse.
- I will not engage in any inappropriate contact or relationship with a client or other participant of the organization's programs.
- I will be alert to any form of abuse from other sources directed toward clients.
- I will not arrange nor participate in any overnight activities (or other prohibited activities) without express permission from the organization.
- I will inform the client's family of any activity plans and obtain their approval as needed.
- I will not buy gifts nor give money to any client. Whenever in doubt of the appropriateness of a modest gift I will check with the organization.
- I will maintain regular contact with my supervisor by responding promptly to any calls, letters, or other means of communication. I also understand that the organization may request a meeting to discuss my participation and I will respond promptly.
- I understand that if a problem arises between the client and/or the client's family or caregiver, I will contact the organization immediately.
- I understand the importance of ending my involvement with the organization properly therefore - I will participate in the organization's exit or termination procedures.
- I agree to follow all established rules and guidelines of the organization
- I have read and agree to abide by the [Name of organization]'s Code of Conduct. I understand that if

I violate this Code of Conduct I will subject to a range of consequences, up to and including being prohibited from participating in any activities or programs of the organization.

Client Code of Conduct

Review the following sample Client Code of Conduct. If your nonprofit does not have a similar policy in place, consider editing this policy to suit your needs.

- I understand as a participant in the [Organization Name]'s program that I am responsible for my behavior.
- I will act in ways that bring respect to me, my family and friends and other participants within the program.
- I will not use bad language, swear, insult or fight with other people. I will refrain from any form of personal abuse towards others, including verbal, physical and emotional abuse.
- I will not engage in any inappropriate contact or relationship with any other participant in the organization's programs.
- I will participate actively in the program.
- I will try new activities and learn new skills to the best of my ability.
- I will not ask to include my friends, brothers, sisters, or other family members in program activities unless they are so invited.
- I will inform my family or caregivers of my program activities. I will not keep secrets about my relationship or activities within the program.
- I will be on time and dressed appropriately for all program activities.
- I will let the organization know if my plans change and I am unable to keep an appointment or participate in an activity.
- I will not expect the staff to buy me gifts, give me money or take me on expensive outings.
- I will ask any staff or other participants if I may call him or her at home. If he/she agrees, I will be reasonable and responsible about the time of day and how often I call.
- I will keep contact with the organization' staff by responding to phone calls, letters and other means of communicating promptly.

If a problem develops, I will immediately talk to my family or caregiver and/or a representative from the organization about it.

If a problem develops within my family or other circumstances occur that affects my participation in the program, I will contact the organization.

- I agree to follow all established rules and guidelines of the organization
- I have read and agree to abide by the [Name of organization]'s Code of Conduct. I understand that if I violate this Code of Conduct I will subject to a range of consequences, up to and including being prohibited from participating in any activities or programs of the organization.

Signature _____Date ____

Interpersonal Relationships

Insert applicable policies about appropriate boundaries here:

Example:

Name of Organization] serves people vulnerable to additional abuse, mistreatment and exploitation. To protect all, we limit contact between our clients and staff (employees and volunteers) to approved activities. Staff should not meet with a client outside the parameters of our organization. Specific limitations are detailed below:

Staff is prohibited from "baby-sitting" for our clients, the clients' families or other participants within the program.

Staff cannot meet with a client and/or the client's family other than during scheduled program

activities.

Staff cannot include anyone other than an authorized employee or volunteer in any program activities involving our clients. Clients cannot include members of their families or friends in any program activities unless specifically permitted.
No overnight visits or activities are permitted without the approval of the organization.
No gifts of a value greater than [insert dollar amount] should be exchanged between staff and clients.
No money should be given to a client and expenditures for program activities should be limited to [dollar amount].

Position Descriptions

NONPROFIT has developed job descriptions for all positions in the organization.

Applications

NONPROFIT uses an application form for paid and volunteer positions.
Insert here applicable policies on interviewing, hiring, reference checking and selecting the most appropriate staff members (and volunteers) for open positions.

Criminal History Background Checks

Insert here applicable policies on background check.

Examples:
" NONPROFIT conducts criminal history background checks on all applicants for positions that will have close contact with vulnerable clients."
or

"It is the policy of our organization to conduct criminal history background checks on all applicants for paid and volunteer positions. The results of these checks are reviewed against the organization's eligibility criteria to determine whether any applicants must be excluded due to the results of the background check."

Emergency Procedures

Insert here a statement about applicable Emergency Procedures such as:

"To ensure the safety of our clients, and staff, NONPROFIT has established an emergency action plan. The emergency action plan is a way for the agency to prepare and plan for various emergencies. All personnel are responsible for knowing and following the plan. Each facility must schedule and hold emergency drills to test the plan and ensure its readiness in the event of an emergency."

Insert here applicable policies about facility security -- include playground security if applicable, and policies relating to confidentiality of facility locations. This would also be the place to describe aspirational future policies/action steps to enhance security policies, such as changes to building access controls.
Insert here any applicable policies about how clients/service recipients are expected to conduct themselves, and the consequences (termination of services?) for a client's failure to follow policy/guidelines for their conduct.

Training and Supervision

Insert here a description of any applicable policy with regard to providing training and supervision of staff in order to protect the safety of the clients served by NONPROFIT.

Financial Management

Financial Responsibilities and Objectives
It is the responsibility of the Board of Directors to formulate financial policies and review the operations and activities of NONPROFIT on a periodic basis. The Board delegates this oversight responsibility to the Finance Committee, of which the Treasurer is the Chair. The CEO of the organization acts as the primary fiscal agent, with responsibility for implementing all financial management policies and procedures on a day to day basis. The CEO may delegate to qualified professional staff responsibility for managing various aspects of financial management.
The financial management objectives of NONPROFIT are to:

- preserve and protect financial assets needed for mission critical activities;
- exercise appropriate care in the handling of incoming funds and disbursement of outgoing funds;
- strive for transparency and accountability in fiscal operations.

Budgeting Process
The CEO, CFO and Treasurer (Finance Committee Chair) shall be responsible for developing and presenting to the Finance Committee a proposed budget for the upcoming fiscal year no less than 60 days prior to the beginning of the new fiscal year. The Finance Committee shall review and approve the budget and present it to the board no less than 30 days prior to the beginning of the new fiscal year. The budget shall contain detailed projections for revenues and expenditures as well as cash flows.

Financial Statements
Insert here language about the periodic review of financial statements such as: The financial committee of the board will review financial statements on a monthly basis and the full board will review the financial statements quarterly. The financial statements will show e a comparison of budget to actual revenue and expenses and also a list of grants or funding that is anticipated but not yet received.

Internal Controls Insert here a description of the internal control policies for NONPROFIT. Example:

[Name of Organization] has adopted a number of internal control measures as part of an overall effort to safeguard financial assets. These controls include:

A policy requiring that all incoming checks are immediately stamped with a restrictive endorsement indicating "for deposit only"
A detailed log of all incoming checks and cash is maintained and reconciled with deposit slips and monthly bank statements
All cash and checks are deposited the same business day if possible, and no later than the next business day
In addition, and to the extent possible given its size and circumstances, the organization strives to to segregate the following duties so that a single staff member isn't required to perform two or more of the following incompatible functions:

Authorizing the purchase of goods and services;
Preparing a purchase order to purchase goods;
Receiving goods or validating the performance of services;

Approving the payment of accounts payable for goods and services received;
Recording the liability for accounts payable;
Preparing and signing checks to pay the respective accounts payable;
Forwarding payments to the payee.

Audit
It is the policy of NONPROFIT to engage the services of a reputable, independent CPA firm to conduct an annual audit of the organization's financial statements. The audit is required to be completed within six months of the end of each fiscal year. The audit firm is selected by and reports to the organization's Audit Committee. A representative of the audit firm is requested to make an annual presentation to the Board of Directors as part of the report by the Audit Committee.

Investment Policy
Insert here any applicable investment policy language

Add any additional Financial Management Policies

Facility Risks

Facility Needs
NONPROFIT seeks to utilize its resources and assets fully in achieving its mission. The prudent use of facilities and resources is required to protect the safety and well-being of all personnel—including staff, volunteers and service recipients—while safeguarding the organization's financial assets.

Facility Design
NONPROFIT is committed to providing a safe environment for its clients and staff through the appropriate use of its premises whether owned, leased or borrowed. The organization strives to construct or modify each property to most efficiently and effectively provide services to our clients while meeting all required codes and regulations.
Inspections Insert here as appropriate:

(i) To maintain the quality of its facilities, NONPROFIT has adopted an inspections schedule and will respond quickly to any deficiencies identified during the inspections.
or
(ii) To ensure the safety of our operations, NONPROFIT inspects its facilities on a regular basis to ensure compliance with regulations, accreditation standards, and our own principles.

Preventive Maintenance
Insert here as appropriate:

(i) To protect its property, personnel and clients from harm, NONPROFIT will take steps to ensure that the organization complies with manufacturer's recommended guidelines for maintenance and repair of equipment and premises, building codes and safety regulations of all jurisdictions applicable to our facility; and maintains a log of service, repair and replacement.
or
(ii) In order to avert accidents, injuries and property damage and be in position to establish that the organization has fulfilled its duty of care, NONPROFIT will maintain a maintenance schedule, checklists, service logs and repair follow-up sheets for each piece of equipment and for key areas on our premises (e.g., stairways, roofs and floors).
Use the space provided to identify the person or position responsible for monitoring compliance with your preventive maintenance policy and updating the policy as needed. We suggest you word your

statement as follows:

"The Chief Financial Officer of [Organization Name] is responsible for monitoring compliance with the preventive maintenance policy and overseeing its review and updating on a regular basis."

Facility Rental/Lease Policy
NONPROFIT does not rent/lease its facilities to outside groups.

Policy Concerning Invitees
As a facility owner, NONPROFIT is committed to providing outside users of its premises with a safe environment. This commitment includes, but is not limited to meeting building code requirements, making timely repairs, and providing and maintaining appropriate security.
Insert here a statement that addresses NONPROFIT 's use of facilities OWNED by others -- whether for its own programs, or for special events. Two separate statements may be appropriate. Some examples follow:

Using Others' Facilities Policy

[Organization Name] will lease space to provide its services at the best market rate available in the neighborhood near to where our service recipients live and near to public transportation. When drafting or signing a lease agreement, we will consider:

Maintenance and upkeep—who is responsible for general upkeep: trash pickup, repairing broken steps, and clearing snow or ice
Mutual indemnification—a contract clause that assures that each party only assumes legal responsibility for those areas or activities under its control
Instructions on the use of property and facilities—detailed directions on how special features operate (e.g. alarm system, fire escape, window air conditioner) and what to do if problems occur
Limits on accessible areas—if the organization is only using a part of the premises, or if certain areas are off limits (e.g. roof, basement, parking lot/garage, outbuildings)
Potential hazards—specific warnings about dangerous or hazardous conditions on the premises
Delegation or supervision—when the landlord/owner chooses to provide staff to assist with supervision (e.g. lifeguards at a swimming pool)
Alcohol consumption—when alcohol is consumed as part of an event (fund-raiser, holiday party), the organization will determine if it is necessary to obtain a temporary liquor license and whether its current insurance is sufficient to cover the event
The organization will spell out its requirements and negotiate the most favorable agreement possible. The organization will seek legal review prior to entering into a lease, whether the arrangement is for a long-term or short-term occupancy.

Using Others' Facilities Policy
[Organization Name] will only use others' facilities for special events, or in an emergency up to and until its facilities are inhabitable once again. The organization will be certain to:

have a written agreement signed by representatives of all parties that spells out the organization's requirements, expectations and responsibilities with regard to the space; this may be a mutual aid agreement in the event of an emergency situation.
fulfill its obligations as spelled out in the agreement and leave the site as tidy as it was found.
supervise its employees, volunteers and service recipients when they use the facility.
refrain from serving alcoholic beverages in facilities being used in the name of the organization.
obtain and review appropriate insurance coverage to cover injury, illness and property damage.

Insert here any policies pertaining to programs that are home-based, such as home visits, if applicable.

Emergency Planning Policy

It is the policy of NONPROFIT to promote good health, well-being and occupational safety for its employees, volunteers and service recipients. Emergency situations require the participation of all staff. Everyone must be familiar with emergency operations. Certain responsibilities are defined to ensure smooth operations. The emergency plan must be readily available, posted in a prominent location, and reviewed annually by the organization's senior management.

Technology and Information Management

Insert here NONPROFIT's policies pertaining to the use of computers and other technology by staff (and clients, if applicable). An example follows:

NONPROFIT's information and office technology systems (networks, software, computers, telephones, printers, copiers, etc.) are tools provided to employees and volunteer to enhance productivity and performance on the job. Limited non-business use is permitted when on personal time (e.g. during lunch hour or after work). Regardless of the type of use, employees must not have any expectation of privacy to data, information or files that are created, stored or used on [Organization Name]'s systems. The executive director or his/her designee reserve the right to access the employee's computer or files at any time. Staff are expected to use good judgment in their use of [Name of Organization]'s information and office technology systems, especially electronic mail. Access to all systems, including electronic mail and the Internet, is a privilege, not a right.

Examples of inappropriate uses of technology include:

- Any violation of law or government regulation
- Any unauthorized access to computer systems or networks
- Any use promoting disrespect for an individual, discrimination, or any use constituting a personal attack, including ethnic jokes or slurs
- Viewing, copying or transmitting material with sexual or profane content
- Transmitting harassing or soliciting messages
- Transmitting unsolicited advertising
- Using copyrighted material without permission or legal rights
- Any use for personal financial gain, or in a manner creating a potential conflict of interest for the employee or [Organization Name].
- Defamatory, inflammatory or derogatory statements about individuals, companies or their products
- Any use that constitutes a waste of [Organization Name]'s resources, including network resources
- Sending or forwarding chain letters
- Any use of network systems for recreational games or other recreational purposes
- Any use that involves corruption or destruction of data, including knowingly launching a virus, worm or other malicious software
- The failure to use good judgment or abuse of the organization's policies may result in suspension of privileges or disciplinary action. If any employee discovers he or she has unintentionally violated this policy, that employee should notify his or her supervisor immediately.

Insert here any policy language pertaining to cell phones and other wireless devices.

Safeguarding Equipment and Systems

Insert here any policy language pertaining to backing up computer systems and security of technology systems.

Examples:

To safeguard its office and technology assets, [Name of Organization] maintains a complete inventory of its electronic equipment and computer and technology systems, including hardware, software, media and data. The inventory process includes documentation of how the networks and systems are configured. Responsibility for maintaining the inventory has been assigned to a regular staff member. The inventory is updated at least quarterly or whenever new equipment, media or software are acquired or discarded. The inventory is stored on-site as well as off-premises.

[Name of Organization] is committed to preserving its assets. To expedite recovery from an incident involving the organization's equipment and systems, responsibility has been assigned for establishing and maintaining an inventory and documentation of all systems. The documentation shall include a complete inventory of electronic equipment and computers technology, including hardware, software, media and data. The assigned staff person will update the documentation on a quarterly basis or as warranted by system acquisitions. The inventory will be stored on-site as well as off-premises.
Insert policy language concerning security of technology systems and WHO will be accountable.
Examples:

Name of Organization] is committed to protecting its office technology assets. The organization takes all reasonable steps to protect and safeguard systems and equipment from damage due to power fluctuations, water damage, dust, extreme temperature change and other environmental factors. In addition, the organization guards against threats to due to viruses, worms, malicious software and hackers. The position in the organization responsible for overseeing the security of office systems is [position].

The [Name of Position] is responsible for efforts to prevent an interruption to the organization's operations due to damage to technology assets, including data. The individual in this position will coordinate the development of appropriate policies and security measures to protect these vital assets.
Insert policy language concerning confidentiality and security of documents/client files. Examples:

Due to the nature of our programs, [Name of Organization] has client files with confidential information as well as business records that are proprietary. Therefore it is essential to limit access to certain records to only personnel whose positions require access. Confidential information in paper form will be stored in locked file cabinets and in a locked room during non-working hours. All personnel should use good judgment and common sense in protecting confidential information while in use during business hours. The IT Director will oversee the creation of a system to limit access to electronic records based on duties and responsibilities in the organization. Access will also be protected through the use of passwords. Access will be modified from time to time as work assignments change. Any employee who intentionally obtains unauthorized access to records shall be subject to discipline, up to and including termination. Any employee who accidentally obtains access to confidential records should inform his or her supervisor immediately.

[Name of Organization] maintains numerous files containing personal data, financial information, and other confidential or proprietary information. These files may be in paper or electronic form. The systems administrator will limit access to certain files based upon individuals' responsibilities and job tasks. Confidential documents will be secured in locked filing cabinets. Any employee whose

work requires access to confidential documents should ensure that files are returned to their secure location. Persons who knowingly obtain unauthorized access to confidential information will be subject to discipline, up to and including termination. All incoming employees will be required to execute a Privacy Policy concerning access to and use of confidential information prior to being given access to any confidential information. [Insert policy language re: computer passwords, if applicable.]

Systems Backup Insert policy on backing up computer systems. Example provided.
[Name of Organization] understands the importance of maintaining computer operations in order to deliver services and programs. A major tool to mitigate damage to computer systems is to adopt procedures for creating and storing system backups to enable the organization to quickly restore any lost files or systems.

Backup Guidelines
Monthly—The last work day of each month the network administrator will perform a backup of the entire hard drive/server. The most recent monthly tape will be stored off-site at the administrator's home and the previous months tapes will be stored in a safe deposit box. The tapes will be rotated on an annual basis and tapes replaced every two years.
Weekly—Every Friday the network administrator will perform a full backup. The most recent backup will be stored at the administrator's home and the remaining tapes stored in the safe deposit box. The four tapes are rotated on a monthly basis and to be replaced annually.
Daily—Every evening (Monday through Friday), the network administrator will perform a differential backup. The daily tapes are stored in a fireproof safe within the office. The tapes will be rotated in a weekly basis and replaced every six months.
Testing—The network administrator will perform a test of the backups on a quarterly basis.
Audit—The network administrator will conduct an audit of backup media at least once every six months.

Disaster Recovery Plan
NONPROFIT's clients are dependent upon us and we must be able to meet their needs even if our facilities become inaccessible or suffer damage. To protect both our clients and our operations we shall adopt a disaster recovery plan for the repair, recovery, and restoration of our computer operations. The [name of position] is responsible for the development, maintenance and testing of the electronic disaster recovery plan. A test of the plan is conducted on an annual basis.

Managing Internet and World Wide Web Risks

Internet Security Insert policy language concerning internet security. Examples:

Due to the critical nature of our information systems and network, we will implement the most stringent yet appropriate security measures to protect our information. The [position name] is responsible for devising and implementing our security protocols. The failure of staff to follow these security protocols may result in suspension of privileges or disciplinary action, up to and including termination.

[Name of Organization] is committed to protecting its network and information technology to the greatest extent possible to ensure our ability to provide programs and services to our constituencies. To achieve our objective, the Director of Administration is responsible for establishing our security protocols and training all personnel in the proper use of these measures. All personnel are responsible for following the security guidelines to protect their computers from harm. Staff who fail to abide by these security protocols are subject to discipline up to and including termination of

employment or volunteer service with the organization.

Transportation Risks

Insert policy guidelines on transportation activities. Examples:

(i) Providing transportation services to clients is an mission-critical function. However, the organization recognizes its responsibility to provide safe and efficient transportation. The following rules apply to all drivers and vehicles:
or
(ii) Only people approved and authorized by [Name of Organization] are permitted to driver either an agency owned vehicle or any other vehicle on the organization's behalf.
Agency owned vehicles are not to be driven for personal use without the permission of the executive director or his/her designee.
While driving on behalf of the organization, personal errands should be avoided.
Agency owned vehicles are to be used within the approved guidelines for use.

To protect our clients and staff, [Name of Organization] will restrict the people allowed to drive on behalf of the organization and specify the terms and conditions when driving or providing transportation services is appropriate for the organization.

NONPROFIT is committed to providing a safe environment for its staff and clients. To achieve this goal, anyone driving on behalf of the organization must be approved. All approved drivers must possess a valid driver's license, acceptable driving record, and adequate personal automobile insurance. Insert policy relating to driver training and standards for those driving vehicles as part of their job duties with NONPROFIT:

Examples:

(i) Providing transportation services to clients is an mission-critical function. However, the organization recognizes its responsibility to provide safe and efficient transportation. The following rules apply to all drivers and vehicles:
or
(ii) Only people approved and authorized by [Name of Organization] are permitted to driver either an agency owned vehicle or any other vehicle on the organization's behalf.
Agency owned vehicles are not to be driven for personal use without the permission of the executive director or his/her designee.
While driving on behalf of the organization, personal errands should be avoided.
Agency owned vehicles are to be used within the approved guidelines for use.
or
(iii) To protect our clients and staff, [Name of Organization] will restrict the people allowed to drive on behalf of the organization and specify the terms and conditions when driving or providing transportation services is appropriate for the organization.

Insert here policy language, if applicable, that pertains to how NONPROFIT will monitor/supervise those who drive. Some risk management strategies include:

(i) Periodically checking motor vehicle records—Pulling the MVR at the onset of employment or volunteer service is increasingly common. Consider pulling an updated record on a regular basis for your drivers (more for full-time drivers and less often for occasional drivers).
(ii) Requiring an on-the-road driving test—Consider having a supervisor or other experienced driver

ride with each driver to re-evaluate their skills.
(iii) Confirming medical conditions—Some positions may require annual physicals or an annual update on the driver's Statement of Medical Condition.
(iv) Administering written driver safety tests—You might administer periodic driver safety tests and record the results.
(v) Reviewing accident and incident reports—Review these reports on a regular basis to identify any trends or areas where follow-up is required.

Vehicle Selection Policy
Insert here any other policy concerning motor vehicle use/drivers.

Vehicle Maintenance
Insert policy on vehicle maintenance, including WHO is responsible:

Examples: It is the policy of [Name of Organization] to inspect all vehicles, except personal vehicles, at least monthly. Vehicle operators/custodians are responsible for ensuring vehicles are serviced/maintained according to the manufacturer's recommended schedule. Any safety problems should be reported by vehicle operators/custodians to the fleet coordinator immediately for proper follow-up.

[Name of Organization] has assigned responsibility to a regular staff member who ensures that all agency-owned vehicles are maintained and repaired. The vehicle supervisor oversees maintenance and repair procedures, such as:

Mileage and maintenance log. Each vehicle contains a log book for drivers to record each trip, including the driver, purpose, and miles driven. The book should also document any maintenance or repairs performed.

Pre-trip inspection. A short pre-trip inspection form is completed by the driver before using the vehicle. Drivers are instructed to refer any problems to the vehicle supervisor. The supervisor also inspects vehicles periodically.

Routine maintenance. The vehicle supervisor schedules and documents the routine maintenance of all vehicles (oil changes, tire rotation and replacement, fluids checked).

Maintenance or repair requests. Drivers are instructed concerning the proper way to report maintenance and repair needs (flat tire, broken seat belt).

Accident Procedures
Insert language here relating to procedures staff should follow in the event of an accident. Example:

Any accident involving a motor vehicle driven on [Name of Organization]'s behalf, regardless of severity, location, or fault, must be reported immediately to the law enforcement authority within the jurisdiction where the accident occurred and to the driver's supervisor at [Name of Organization]. Fleet vehicles contain an Emergency Kit with the following: reflective triangles, accident procedures, blank accident report, and first aid kit. In the event a rented vehicle is being used, the driver should also follow the procedures outlined on the rental agreement and/or posted in the vehicle.

All of the organization's drivers have been instructed to follow the following procedure for all accidents:

Stop and secure the vehicle.
Set out warning devices (triangles) properly.
Immediately contact the local police to advise them of the accident and request medical assistance if there are any injuries.
Once any medical needs are taken care of, obtain information on the other driver or drivers involved in the accident. Use the accident form to record this vital information.
Provide the other driver(s) involved in the accident with your information and the vehicle's information, including insurance coverage. Insurance information is located in the Emergency Kit of all fleet vehicles.
Cooperate with the police and other authorities but do not admit fault.
If necessary due to the condition of the vehicle, arrange for towing to a nearby garage.

Crisis Management

Emergency Planning
NONPROFIT views emergency planning as essential to mission fulfillment. The organization's emergency plans reflect input from key organization personnel. Components of the plan include business continuity, crisis communications and facility evacuation.
Business Continuity Planning Policy
The Business Continuity Plan of NONPROFIT will:

- help the organization fulfill its moral responsibility to protect employees, other stakeholders and the community in which we operate
- facilitate compliance with regulatory requirements of federal, state and local agencies
- enhance the organization's ability to reduce its financial losses, regulatory fines, damage to equipment or disruption to service delivery in the event of a business interruption
- reduce exposure to civil or criminal liability in the event of an incident
- enhance the organization's image and credibility with employees, clients, funders, vendors and the community.

Internal Distribution Policy for BCP Policies and Procedures
All pertinent policies and procedures needed to ensure that services are provided during a business interruption will be provided electronically to all senior managers on an annual basis. It is up to these managers to educate their respective staffs about their role in supporting the business continuity plan.

Vital Information Backup Policy Insert here policy language that reflects how NONPROFIT will ensure that vital business documents are maintained and able to be located in an emergency. Examples:

(i) Vital Information Backup Policy
Each department or program will develop procedures to backup vital records, data and documents that are essential to fulfilling the organizational business continuity plan. Each department will assign a lead staff member (and an alternate) to coordinate this task.

(ii) Vital Information Backup Policy
[Organization Name] will develop backup procedures for protecting and preserving paper-only records and documents; electronic documents and data; and staff status availability and notification, including emergency contact information.

(iii) Vital Records, Data and Documents Backup Policy
In order to ensure the continuity of mission-critical services, [Organization Name] will duplicate and store off site all information identified as essential to fulfilling its business continuity plan.

Crisis Communications Policy Insert here policy language pertaining to crisis communication procedures. Strategies may include:

(i) Who might need to be contacted (constituencies served by the organization, groups affected by the organization's operation and those to whom the organization is accountable)?
(ii) How will they be contacted (land lines, wireless, e-mail, runners)?
(iii) What backup systems are available if the primary medium is unavailable (telephone wires down or wireless transmissions overwhelmed)?
(iv) How many people have copies of staff names and contact information and how often is the information updated?
(v) Will one person contact everyone or will a group of people be mobilized?
(vi)Who is in charge of gathering the facts and crafting the official message?
(vii) Who is the official spokesperson and who is the backup in case that person isn't available?
Insert here policies pertaining to emergency evacuation from various facilities, and WHO is responsible for ensuring that residents/staff are aware of and have drills to practice evacuation in accordance with the plan.

Volunteer Risks and Risk Management Strategies

Priority Volunteer Risks
Top Risks relating to Volunteers:

Not having the "right" board members
Volunteer causing harm to clients
Volunteer causing harm to reputation of NONPROFIT

Addressing Risks Through Recruitment, Screening and Selection
Insert here any policy language relating to recruitment and selection of volunteers for programs.

Policies relating to board member recruitment/selection (e.g., criteria for serving on the board) may also be included here.

Insert policy language, as applicable, relating to supervision of volunteers.

Volunteer Dismissal
Insert policy language, if applicable, relating to the dismissal of volunteers. (Dismissal of board members is generally addressed in the bylaws). Example:
Volunteer Dismissal

Volunteers serving [Name of Organization] may be dismissed at any time when a supervisor determines that:

The volunteer is indifferent with regard to the organization's essential rules and requirements;
The volunteer cannot adequately perform the job for which they have been retained;
The volunteer's continued service presents an unacceptable danger to the organization or its personnel or clients.
At the time of dismissal departing volunteers will be provided with a letter thanking them for their past service and explaining the reason why their continued service is no longer required. All volunteer dismissals will be reviewed by senior management in advance of taking action.

Insurance Program for NONPROFIT

Insert here a description of NONPROFIT's insurance-buying strategy and a summary of your current insurance program.

The first line might be: NONPROFIT will investigate the usefulness of a Risk Management Committee to advise the organization about risk management issues including insurance purchasing.

Other examples: "The organization purchases insurance to protect against catastrophic losses.

The Risk Management Committee for the organization works with the Director of Finance to review proposals submitted by qualified brokers and to determine the most appropriate limits of liability, deductibles and carriers given the resources, risks and requirements of the organization.

The current insurance program for [Name of Organization] consists of the following coverages:

Coverage A - Limits of X with Y Carrier (expiration date: 10/31/08)
Coverage B - Limits of X with Z Carrier (expiration date: 12/31/08)

Your entry may be a simple summary or a more detailed description of your process for purchasing insurance.

You may also choose to reference the specific policies by appending a copy of the current "schedule of insurance" which can be obtained from your insurance broker.

Insurance Advisors
Insert here a statement of what NONPROFIT expects from its insurance professional.

With respect to an organization's agent or broker, the first expectation is that he or she will help your organization purchase adequate insurance coverage at an acceptable price. However, beyond that basic service, what can you expect from your insurance professional? Additional services can include:

(i) claims management assistance in reporting and handling claims and acting as your advocate;
(ii) premium and loss reports on a periodic basis;
contract review for insurance implications;
(iii) loss-control and prevention activities;
risk management services;
(iv) educational resources, for example, provide training sessions for employees, volunteers and the board of directors;
(v) account reports and updates throughout the year;
(vi)annual stewardship report; and
client advocacy and business partnership.

Insert here a statement that describes NONPROFIT 's approach to working with an insurance professional to review its insurance program. Examples:

(i) NONPROFIT puts its insurance program out to bid every 3-5 years, or more frequently if the organization determines that a current provider is unable to meet the service needs of the organization.

(ii) It is the policy of [Name of Organization] to evaluate the performance of any and all insurance advisors (agents or consultants) on an annual basis and seek competitive bids for these services no

less than every five years. The incumbent advisor will be invited to participate in the bidding process as long as their current performance meets the minimum requirements of the organization.

Insert here information on current insurance professional(s). Example: NONPROFIT has retained the services of XYZ Broker effective July 1, 2008. The deliverables due to ABC are outlined in a Broker Services Agreement. ABC pays a fee for these services and any quotes obtained from carriers are presented net of commission.

Additional Risk Management Policies

Insert here any special risk management policies that pertain to the Gala/fund raising events.

Examples:
(i) Having a back-up plan for speaker/honorees in the event the speaker cannot attend
(ii)Need to diversify advertising spots beyond one newspaper
(iii) Special Fundraising policies: Need to develop a policy on gift acceptance and educate the board on gifts that NONPROFIT will/will not accept and on restricted gifts
(iv) Evaluate whether Special Event Insurance would be appropriate.

Insert here copies of critical HR policies as well as a plan for action steps to develop policies that will help keep staff safe and that address quality workplace issues:

(i) insert Anti-Harassment Policy - ADD schedule for periodic review of policy
(ii) NEED to develop a Whistleblower Protection Policy
(iii) insert Grievance Policy - ADD schedule for periodic review of policy
(iv) insert relevant Confidentiality policies such as Board policy on confidentiality and confidentiality of client information
(v) NEED to develop policy on collecting personal financial information; and
(vi) review the need for a policy addressing client obligations re: confidentiality.
(vii) NEED to develop formal policies for review of compensation of ED.
(viii)insert policy language to reflect that NONPROFIT regularly reviews comparable salary and benefit information in order to evaluate whether its own staff salary administration is consistent with retaining and motivating staff and also with budget realities.
Insert here statements about goals for risk management policies in the governance and leadership area, such as:
(i) Develop a leadership succession plan (by when? who is responsible?)
(ii) Periodically review the board's composition to ensure that the board provides the expertise, experience and commitment needed to forward the mission. Consider developing written guidelines for board eligibility. Consider developing a statement on commitment to board diversity.
(iii) Conduct an annual board self-evaluation (by when? who/what committee is responsible?)
(iv) Consider implementing a Risk Management Committee
(v) Consider using a "consent agenda" format for board meetings to move along the agenda and ensure adequate time for engaging the board in important policy discussions.
(vi) ADD policy statements about NONPROFIT's commitment to board orientation and training (when? who is responsible?)