CASA
Court Appointed Special Advocates
FOR CHILDREN

KENAITZE INDIAN TRIBE,
COURT APPOINTED SPECIAL
ADVOCATE PROGRAM

Kenaitze Indian Tribe CASA Program PO Box 988 Kenai, AK 99611 (907) 283-3633 ext 290 kmiller@kenaitze.org

KENAITZE INDIAN TRIBE CASA
RISK MANAGEMENT PLAN

June 30, 2009

Adapted from NCASAA business Risk Management Template

Risk Management Plan

The Kenaitze CASA Program has created a risk management plan that addresses risks and treats the program may face. The risk management plan was complied with the participation from all staff of Kenaitze CASA and its volunteers to ensure diverse perspectives are included in the plan. By participation staff and volunteers will also have a clear idea of what is expected from them and that they will understand their responsibilities. The risk management plan will also face Tribal Council vote and approval.

General Safety Principles

- Kenaitze CASA will to the best of our ability operate in compliance with all laws, local, federal and state. Kenaitze CASA also honors and practices all the standards set forth by National CASA Association.

- Volunteers and staff are thoroughly screened, selected and trained. At no time shall any CASA staff or CASA volunteer transport a child or meet with a parent of a child who is assigned a CASA in his or her car.

- Kenaitze CASA through the tribe has existing policies that are enforced, standards that are understood and followed, guidelines that are set forth and procedures that are clear.
- Kenaitze CASA will maintain safe and secure facilities and practices. In the event of an emergency a clear plan is set in place.
- Channels for communication in the event of incidence, emergency or concern are clearly communicated to all employees and volunteers.
- A written conflict of interest policy is kept in all staff and volunteer files, reviewed yearly and new policies are adopted and reviewed on a yearly basis.

Responsibility for Risk Management

Tribal Council
- Establishes risk management goals, objectives and the operating budget
- Reviews all complaints, reports to set futures goals of the program
- Approves goals and standards of the program

Legal Counsel for the Organization
- Legal Advisor/Representation on legal matters as they arise

Executive Director and Human Resources
- 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 Tribal Council aware of new and continuing risks.
- Reviews the organization's insurance program periodically.
- Reviews the organization's risk management plan annually.
- Evaluates the insurance program and that insurance is in place for the Tribe.

Program Director and Coordinator
- Ensures compliance with protocols and standards set by the National CASA Association.
- Oversees the assets of the Kenaitze CASA program and ensures protection thereof.
- Periodically meets to review organization risks and achievements with the Executive Director.

Insurance Program for Kenaitze CASA Program

The appropriate insurance is held with the Human Resources Department for the whole Tribe and all employees and volunteers.

Human Resources

Policies, procedures and written employee rules of conduct are given and signed by the employee or volunteer at the time of new hire orientation and Kenaitze badges are also issued at this time.

Communications Regarding Employment Policies

New policies are communicated verbally and in writing to all employees and volunteers.

Kenaitze CASA Program reviews and updates its employee policies yearly. Compliance with state and federal employment laws are adhered to.

Kenaitze CASA Program uses job descriptions for both paid and volunteer positions in the organization. These documents are reviewed and updated on an as needed basis and kept in the personnel files.

Staff Supervision

Kenaitze CASA is and maintains compliance with the National CASA Association standards regarding supervision. Staff supervisors also perform evaluations of all employees and volunteers every six months and are kept in personnel files.

Financial Management

Financial Responsibilities and Objectives

Financial responsibility is shared between the Executive Director, Director of the program, Accounting Manager, Program Coordinator and the Chief Financial Officer. Day to day financial management is the responsibility of the program coordinator. On a monthly basis the accounting manager submits required reporting and financial statements to National CASA Association and the Executive Director of Kenaitze Indian Tribe. Monthly the Tribal Council and Executive Director meet to approve new requirements and/or discuss needed changes to the program and the risk management plan.

Budgeting Process and Internal Controls

October of every year the Tribal Council has its annual meeting and a new or revised budget for the CASA program is voted on and/or adopted. Internal controls concerning the program are also discussed and improved as need during the annual meeting.

Audit

The Tribal Council requires an annual audit to be completed and conducted by an outside Audit agency approved by the Tribal Council. The audit must be completed between three to six months after the fiscal year has ended.

Gift Acceptance Policy

Gifts and donations will be made in accordance with the approved Kenaitze Indian Tribal Council Budget(s) set aside for this purpose. All items over $500.00 will be brought to the Council for prior consideration and approval.

All Federal and State Laws regarding gifts and donations will be adhered to. Grant compliance will be adhered to.

All gifts of donations will be handled using general fund practices and the required reporting set forth by the donor or giver will be honored and adhered to.

Building Facility Risks

Operational and building design support is given to all occupants. The Kenaitze Indian Tribe strives at all times to make sure that its facility is up to standards and code on the local, state and federal level. Regular repair, maintenance, upgrade and logs of all activity are performed on a regular basis.

Policy Regarding the Use of Others' Homes or Apartments

Kenaitze CASA will not be engaging in the use of others' homes or apartments for any official business or activity.

Emergency Planning Policy

At times, emergencies such as but not limited to severe weather, fires, power failures, or earthquakes, may disrupt Kenaitze Indian Tribe operations. In extreme cases, these circumstances may require the closing of your work facility. This decision will be made by the Executive Director. In the event that such an emergency occurs during nonworking hours, local radio stations will be asked to broadcast notification of the closing.

A copy of emergency procedures and handling procedures is kept on file with Human Resources and all employees and volunteers are informed at the time of hire/orientation.

Information Management

Cell Phone Usage

Kenaitze Indian Tribe provides cellular telephones to some employees as a business tool. They are provided to assist employees in communicating with management and other employees, their clients, associates, and others with whom they may conduct business. Cell phone use is primarily intended for business-related calls. Employees should not rely on KIT cell phone for regular personal use, and personal cell phone calls are to be curtailed during working hours.

KIT cell phone invoices will be regularly monitored. Cell phone availability is dependent upon program funding and grant restrictions.

Employees may have access to a cell phone while in their cars and should remember that their primary responsibility is driving safely and obeying the rules of the road. Employees are prohibited from using cell phones to conduct business while driving and should safely pull off the road and come to a complete stop before dialing or talking on the phone.

As a representative of KIT, cell phone users are reminded that the regular business etiquette employed when speaking from office phones or in meetings applies to conversations conducted over a cell phone.

Computer and Email Usage

Computers, computer files, the email system, and software furnished to employees are KIT property intended for business use. Employees should not use a password, access a file, or retrieve any stored communication without authorization. To ensure compliance with this policy, computer and email usage will be monitored.

KIT strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, KIT prohibits the use of computers and the email system in ways that are disruptive, offensive to others, or harmful to morale.

For example, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off color jokes, or anything that may be construed as harassment or showing disrespect for others.

Email may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters.

KIT purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, KIT does not have the right to reproduce such software for use on more than one computer.

Employees may only use software on local area networks or on multiple machines according to the software license agreement. KIT prohibits the illegal duplication of software and its related documentation.

Employees should notify their immediate supervisor, the IT Department or any member of management upon learning of violations of this policy. Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.

Internet Usage Policy

Internet access to global electronic information resources on the World Wide Web is provided by KIT to assist employees in obtaining work-related data and technology. The following guidelines have been established to help ensure responsible and productive Internet usage. All Internet usage is limited to job-related activities. Personal use of the Internet using KIT's accounts and computer equipment shall be limited to non-working hours and is subject to this policy.

All Internet data that is composed, transmitted, or received via our computer communications systems is considered to be part of the official records of KIT and, as such, is subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical, and lawful.

The equipment, services, and technology provided to access the Internet remain at all times the property of KIT. As such, KIT reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, or received through our online connections and stored in our computer systems.

Data that is composed, transmitted, accessed, or received via the Internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it, or has not gotten authorization for its use, it should not be put on the Internet. Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights.

Internet users should take the necessary anti-virus precautions before downloading or copying any file from the Internet. All downloaded files are to be checked for viruses; all compressed files are to be checked before and after decompression.

Abuse of the Internet access provided by KIT in violation of law or KIT policies will result in disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organization's time and resources for personal gain
- Stealing, using, or disclosing someone else's code or password without authorization
- Copying, pirating, or downloading software and electronic files without permission
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization

- Violating copyright law
- Failing to observe licensing agreements
- Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions
- Sending or posting messages or material that could damage the organization's image or reputation
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals
- Attempting to break into the computer system of another organization or person
- Refusing to cooperate with a security investigation
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Using the Internet for political causes or activities, religious activities, or any sort of gambling
- Jeopardizing the security of the organization's electronic communications systems
- Sending or posting messages that disparage another organizations products or services
- Passing off personal views as representing those of the organization
- Sending anonymous email messages
- Engaging in any other illegal activities

Safeguarding Equipment and Systems

Policy on Systems Inventory and Documentation
Yearly an audit of all internal and external assets is completed by the accounting clerk. An audit ensures Kenaitze CASA program protects and secures all its assets.

Protecting Confidential Information
Kenaitze Indian Tribe will protect the confidentiality of employees, clients, and Tribal members. All persons working, volunteering, or doing business with Kenaitze Indian Tribe, both during and after the time such engagement has been completed or terminated will be subject to KIT's confidentiality policy. This policy prohibits confidential information as defined by Federal (such as the Health Insurance Portability & Accountability act) and State laws and regulations, from being accessed, disclosed, or released in any format to or by any person/party that does not have a "need to know" without the proper consent of the individual involved, and/or the Kenaitze Indian Tribe. In addition, certain information considered confidential by KIT may not be released without specific authorization from the appropriate level of management (Executive Director or Tribal Council).

Conduct of Personnel: All employees are expected to maintain confidentiality at all times, whether dealing with conversations, records, or projects. Violations of this policy may include, but are not limited to:

- "Loose talk" or gossip regarding medical or other personal information about any patient, client, or fellow employee.
- Allowing unauthorized access on KIT computers to confidential client/patient information, financial data, research data, or employee personal information.
- Sharing of information acquired by persons in the course of their work to others who do not have a need to have the information; accessing information that an individual doesn't have the authority to access in the course of their work, or doesn't need to know to carry out their job duties.
- Disclosure of the anonymity or medical information of research participants without the research subject's permission.
- Sharing of information relative to confidential Human Resources matters.

- Breach of confidentiality obligations with regards to information that is subject to a specific confidentiality agreement.
- Discarding confidential documents in a non-secure manner (failure to shred, confidential materials when discarding).
- Failure to store confidential materials and records in a secure, locked file; leaving confidential materials where they may be inadvertently viewed by persons who are not covered by "need to know".

Examples of Types of Information to be Protected:

1. Client/Patient Information – Client/patient information must not be accessed, removed, discussed with or disclosed to unauthorized persons, either within or outside of the specific department or KIT, without the proper consent of the client/patient. All individuals having access to confidential information are bound by ethical and legal restrictions on the release of medical/psychosocial data. No individual therefore may disclose to a third party, including his/her own family, information learned from medical records, patient accounts, management information systems, or any other confidential sources during the course of his/her work. No individual may access confidential information that they do not need to know to carry out their job duties. Employees may not access, release, or discuss the medical information of other employees without proper consent, unless the employee must do so to carry out specific job functions. Employee patient information should never be accessed for employment reasons. Employees may not access their own medical, billing, or scheduling information except through the customary approved channels for patients.

2. **Kenaitze Indian Tribe Information -** KIT information that must be protected includes but is not limited to:

    - Ongoing negotiations (contracts, leases, purchases)
    - Pending litigation and/or investigations
    - Information that is proprietary; e.g., information which allows KIT to be more competitive in the marketplace, for example an innovative approach described in a grant or contract proposal.
    - Confidential financial or commercial information
    - Information that was discussed under an oath of confidentiality, for example in an Tribal Council Executive (closed) Session or Grievance Committee hearing.

This information may not be accessed, removed, altered or disclosed unless KIT administration has given proper authorization.

3. **Individual Matters and Program- Specific –** This includes personnel, medical, and other similar files where unauthorized access or release, falsification or destruction of confidential individual records is strictly prohibited. Each department manager is responsible for developing and maintaining confidentiality procedures responsive to grant and program regulations (e.g. Head Start, ICWA, mental health etc.) and ensuring employees are oriented to program-specific procedures.

Disposal of Confidential Documents:
Disposal of confidential documents shall be through shredding on site at KIT offices.

Reporting Breach of Confidentiality
Persons must report violations of this policy to their direct supervisor, department manager, or Executive Director.

Exceptions:

Mandatory reporting as required for their protection of minors, elders, and vulnerable adults under AS47.17.010 and AS47.24.010 ARE AN ALLOWABLE EXCEPTION TO CONFIDENTIALITY UNDER Alaska law. Each employee is required to consult their respective department operating policies and procedures for these and any other exceptions to confidentiality.

Confidentiality Agreement:
Each employee, volunteer, Tribal Council member, and contactor will be required to sign a Confidentiality Agreement prior to performing any functions for Kenaitze Indian Tribe.

Confidentiality Statement for Clients
Each program or department will provide a confidentiality statement compliant with all applicable regulations governing that program, to patients, clients, or participants, at the time of engagement of KIT services.

Disciplinary Action for Non-compliance
Violation of this policy is cause for disciplinary action up to and including dismissal.

Use of Passwords as a Security Measure
Computer and phone passwords are required by Kenaitze Indian Tribe and are to be changed every three months or as directed by the IT manager.

Systems Backup
System backup and disaster recovery are very important to Kenaitze CASA and Kenaitze Indian Tribe. It is the responsibility of the IT manager and Executive Director to oversee backup and recovery. Upon completion of every work day a full backup is completed and information is stored off site in a secure location.

Crisis Management

Crisis Communications Policy

A preemptive approach to a public media crisis is ensured by the Tribe. No one is allowed to speak to the media without the expressed written consent or permission of the Executive Director of Kenaitze Indian Tribe. At times there may be a designated spokesperson authorized to speak on behalf of the Tribe and/or Kenaitze CASA. At no time will Kenaitze CASA confirm its involvement or lack of involvement with a child in need of aid case.

Special Accommodation
Any person(s) who required special accommodations will be known to all staff members and all specified needs will be provided to ensure the person(s) safety and that they are able to perform their job duties without restraint. Kenaitze CASA will evaluate on an individual basis all persons wishing to become a volunteer to see if the work as an advocate is appropriate for the person or the Tribe.