Chapter 200. FINANCIAL POLICIES

§212 Fraud Policy

§212.1

District Management is responsible for the detection and prevention of fraud, misappropriations, and other irregularities. Fraud is defined as the intentional, false representation or concealment of a material fact for the purpose of inducing another to act upon it to his or her injury. Each member of the management team will be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of irregularity. Any fraud that is detected or suspected must be reported to the District Manager or alternatively, to the chair of the Financial Committee, who coordinates all investigations.

§212. 2 Actions Constituting Fraud

The terms fraud, embezzlement, misappropriation, and other fiscal irregularities refer to, but are not limited to:

a) Any dishonest or fraudulent act

b) Forgery or alteration of any document or account belonging to the District

c) Forgery or alteration of a check, bank draft, or any other financial document

d) Misappropriation of funds, securities, supplies, equipment, or other assets

e) Impropriety in the handling or reporting of money or financial transactions

f) Disclosing confidential and proprietary information to outside parties

g) Accepting or seeking anything of material value from contractors, vendors, or persons providing goods or services to the District

h) Destruction, removal or inappropriate use of records, furniture, fixtures, and equipment

i) Any similar or related irregularity

§212.3 Investigation Responsibilities

The District Financial Committee has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. The Finance Committee may utilize whatever internal and/or external resources it considers necessary in conducting an investigation. If an investigation substantiates that fraudulent activities have occurred, the Financial Committee will issue reports to the appropriate personnel, and if appropriate, the District Board of Trustees. Decisions to prosecute or refer the investigation results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in conjunction with legal counsel and senior management, as will final dispositions of the case.

Chapter 200. FINANCIAL POLICIES

§212.4 Confidentiality

The Financial Committee will treat all information received confidentially. Any employee who suspects dishonest or fraudulent activity will notify the District Manager or the Financial Committee Chair immediately, and should not attempt to personally conduct investigations or interviews related to the suspected fraudulent act. (See Reporting Procedures in section 212.6) Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the District from potential civil liability.

§212.5. Investigation Authority

Members of the District Financial Committee will have free and unrestricted access to all District records and premises and authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without the prior knowledge or consent of any individual who may use of have custody or any such items or facilities when it is within the scope of their investigations.

§212.6 Reporting Procedures

Care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

An employee who discovers or suspects fraudulent activity will contact the District Manager or the Chair of the Financial Committee immediately. Alternatively, the employee may use the Employee Risk Management Authority (ERMA- this is a part of the VCJPA self-insurance group coverage) Employee Reporting Line at 1-877-651-3924 to make an anonymous report. This line is monitored 24 hours a day. The employee or other complainant may remain anonymous. All inquiries concerning the activity under investigation from the suspected individual(s), his or her legal counsel or any other inquirer should be directed to the Financial Committee or legal counsel. No information concerning the status of an investigation will be given out. The proper response to any inquiry is “I am not at liberty to discuss this matter.”

The individual making the report should be counseled to not contact the suspected individual in an effort to determine facts or demand restitution and to not discuss the case, facts, suspicions, or allegations with anyone unless specifically asked to do so by the District legal counsel or Financial Committee.

§213 Accounting Security

Petty Cash is stored in a locked file cabinet. The Administrative/Financial Manager and the District Manager will be the only employees with keys to the Petty Cash cabinet.

Chapter 200. FINANCIAL POLICIES

§214 Access to Electronically Stored Accounting Data

It is the policy of the District to utilize passwords to restrict access to accounting software and data. Only duly authorized accounting personnel with data input responsibilities will be assigned passwords that allow access to the system.

§215 Storage of Backup files

It is the policy of the District to maintain back-up copies of electronic data files off-site in a secure fire-protected environment. Access to back-up files shall be limited to individuals authorized by management.

§216 General Office Security

During normal business hours, all visitors are required to check in at the front counter. After hours a key and security passcode are required for access to the District's office. Keys are issued only to employees (and janitorial services).

§217 WARRANT AUTHORIZATION SIGNERS

Warrant Requests require two signatures from the following group, Board Members, District Manager and Field Operations Supervisor (when District Manager is unavailable).

§218 ELECTRONIC FUNDS TRANSFERS

District Manager is authorized to transfer funds between LAIF, County account and VCJP. District manager will get preapproval from the Board at the previous meeting. Approval noted in Board Minutes.

§219 CASH RECEIPTS

When miscellaneous checks come in the mail Administrative/Finance Manager will prepare a County deposit form and mail to County with the check. The District keeps a copy of the check for records. Enter all revenue into accounting software once a year.

§220 BANK AND CASH ACCOUNT RECONCILIATIONS

LAIF and VCJPA statements reconciled once a year at the end of the year. County cash general ledger detail is reconciled as soon as it is received. Payroll imprest account is reconciled monthly.

§221 CREDIT CARDS

Seven support staff have a credit card. Employees can purchase items approved in the budget. Receipts are given to Administrative/Finance Manager. The receipts are reconciled to the statements and then recorded to the general ledger. Disbursement goes through the warrant process noted above.

§222 CAPITAL ASSETS

Administrative/Finance Manager maintains a capital depreciation schedule. Items over $5000 are placed on the depreciation schedule.

Chapter 200. FINANCIAL POLICIES

§223 PAYROLL AND BENEFITS

The District uses ADP for payroll. Payroll is paid bi-monthly. ADP prepares 941 and DE6 forms. ADP delivers payroll checks to the District. Employees have option to have direct deposit handled by ADP. Administrative/Finance Manager records payroll to the general ledger twice a month. Payroll is paid out of a separate imprest bank account. Employees enter time into VCMS system. VCMS reports are reviewed monthly by the management staff. Administrative/Finance Manager prepares an Excel payroll spreadsheet that is approved and signed by the District Manager. This report is support for the transfer of funds from the County cash account to the payroll account.