POLICY 8.7 WHAT THE DISTRICT EXPECTS

ADOPTED: FEBRUARY 1, 2013 REVISED:

A. TEAMWORK AND EXCELLENCE

This section has been arranged to present a general overview of some of the District's expectations of its employees. Every employee should keep in mind that each is a part of a team of public employees, and public satisfaction with the District depends upon good service.

B. PERSONAL CONDUCT

Positive attitude, proper courtesy, and conduct on and off the job are important to the individual as well as to the District. Neatness of work performed is also important. All employees are engaged in public relations. Some deal directly with the public; others, while not in direct personal contact, do perform work under the public eye. Employees of the District, regardless of whether contacts are direct or indirect, are expected to be courteous, efficient, and helpful in all their work assignments. Favorable impressions created by employees' public behavior help develop good will and support for District services.

C. CODE OF ETHICS FOR DISTRICT EMPLOYEES

1. Personal Interests Avoided. District employees may not use District time, equipment or services for personal interest or gain. When giving testimony unrelated to their assigned District responsibilities, District employees shall not use information or facts that have come to them by virtue of their employment for personal gain or benefit. In matters of personal interest, employees should conduct themselves so as not to impair their working relationship with other employees, officials, or the public.

2. Gifts and Gratuities. Employees shall not accept any special favors, gifts, or gratuities resulting from or related to employment with the District. In this regard, the appearance of impropriety can be as damaging as actual impropriety and shall be avoided.

3. Special Gifts. Department heads may allow acceptance of non-monetary gifts of nominal value [e.g., under $50] at holidays or special occasions which are available to be shared by all employees.

4. Chain of Command Financial Reporting. Jefferson Rural Fire Protection District is committed to creating an environment where fraudulent and other dishonest acts are not tolerated. This policy establishes responsibilities for investigating potential incidents of fraud or other dishonest acts, taking remedial actions, and reporting evidence to the outside Auditor and other appropriate authorities.

5. Jefferson Rural Fire Protection District operates under the direction of Board of Directors. District employees are subject to all provisions of Board Policy *Code of Ethics For District Employees.* The policy requires that state resources entrusted to the District must be used for their dedicated purpose. Dishonest and unethical acts by employees are prohibited. If such acts are reasonably suspected by an employee, they shall be reported through the employee's supervisor to the Fire Chief. If the Chief is unavailable, the Chain Of Command Policy should be followed. If the employee is uncomfortable reporting the incident to their supervisor, the incident may be reported to the Business Office Manager, or the Chair of the Finance Committee. The Board President, or designee, shall investigate such report. Employees shall not make statements or disclosures in reckless disregard of truth.

6. Alcohol - Illegal or Recreational Drugs
   a. No Alcohol or Illegal or Recreational Drugs shall be brought onto or into any fire district property for the purpose of consumption.

   b. No Alcohol or Illegal or Recreational Drugs shall be transported in any fire district vehicle.

   c. No Alcohol or Illegal or Recreational Drugs Drug shall be consumed on or in any fire district property.

   d. No one will respond to any district function or emergency on district property after consuming any alcohol - Illegal or Recreational Drugs.

   e. The chief will address any judgmental variance.

7. <u>Firearms and Fireworks</u>
   a. No Firearms or Fireworks shall be brought onto or transported in any district property. (unless official fire district business)

   b. No live Ammo shall be brought on to or transported in any district property. (unless official fire district business)

   c. No firearm shall be discharged on or in any district property.

   d. Exception: If firearm is require as part of a person's job and has a handgun permit and has cleared it with the Fire Chief may carry when needed only.

8. <u>Inappropriate Language or Visual Aids.</u>
   a. No language that offends anyone or makes anyone uneasy shall be used during district functions or emergencies, especially in public areas.

   b. No humorous stories or visual materials that offends anyone shall be allowed on or in any district property.

c. No pornography, either written, audible or visual shall be allowed on or in district property.

d. No district computer shall be used to view, download or order any materials that are considered inappropriate.

e. No district airwaves, either hard line or cellular shall be use to contact any company or agency that would distribute any inappropriate material.

9. Tobacco Use

No tobacco use of any kind shall be permitted on district property, drill site or district vehicle. Special circumstances may be granted by the chief only.

10. Sexual Activity

a. No Sexual activities shall be permitted on district property or in any district vehicle.

b. No one under the age of 18 shall be permitted to enter any room that is designated to be or is assigned as a bedroom or sleeping quarters.

c. No one, no matter what their ages, shall be allowed to spend the night in any district property. Exceptions are student sleepers, ambulance crews or ambulance riders. Any other exception shall be cleared by the Station Captain or above. The station Captain must inform the Chief of their decision and why.

11. District Apparel

a. Fire District Apparel shall not be worn into any establishment that reflects negatively on the fire district. District apparel shall not be donated to any used apparel stores. All used apparel will be destroyed or returned to the district.

b. No one shall attempt to use uniforms, badges or any official uniform pieces to gain financially or physically by their use.

c. You shall, while wearing district apparel, act and represent the Jefferson Fire District in the highest possible professional manner.

D. POLITICAL ACTIVITIES OF DISTRICT EMPLOYEES

1. Official Position - Campaigning. Employees may not use their official authority or position with the District to further the cause of any political party or candidate for nomination or election to any political office.

2. On-Duty Activity. Oregon law forbids any District employee, while on the job, from soliciting money, influence, service, or other article of value or otherwise aiding and/or promoting any political cause or the nomination or election of any person for public office.

E. COST CONSCIOUSNESS

Every employee of the District is a citizen and taxpayer and is expected to practice economy in all duties. Failure to do so is not in the best interests of the District and may lead to discipline, and/or discharge, as appropriate.

F. ATTENDANCE AND PUNCTUALITY

Each employee and the employee's performance on the job are important to the overall success of operations. When absent, someone else must do the job. Everyone is expected to keep regular attendance, be on time, and work as scheduled.

In accepting employment with the District, each employee is required to meet certain standards. Maintaining an acceptable level of job attendance is part of good work performance and is one of the standards by which an employee's overall contribution to the District may be measured. Continued employment carries with it the personal responsibility of each employee to be on the job on time every scheduled work day. Recurring and excessive absences and/or tardiness are disruptive to work schedules, costly to the District and its residents, and detrimental to the morale and efforts of employees who maintain a good work record.

Except when the absence is due to leave protected by state or federal law, failure to meet these requirements subjects an employee to disciplinary action, which include termination. The ability to attend work regularly is a job requirement.

G. PERSONAL APPEARANCE

Each employee is responsible to present a proper, businesslike appearance whether in the office, a District vehicle, or other site. Good taste and good judgment in personal attire is expected.

H. APPEARANCE OF WORK AREAS

The District's objective is to provide and maintain clean, safe and healthy work conditions. It is the responsibility of each employee to maintain a safe, neat work area and insure that all working documents, desks, cabinets and equipment are secure at the close of the work shift**.**

I. PERSONAL TELEPHONE CALLS

District phones are to be used for District purposes. Telephone calls of a personal nature (incoming or outgoing) should be kept to a minimum and made during breaks or lunch periods whenever possible. Under no circumstances should an employee charge a long distance call to the District unless it is work-related. Friends and relatives should be discouraged from calling during working hours except in emergencies.

J. SMOKING

The District prohibits smoking within all District buildings and pursuant to the Oregon Smoke Free Law, ORS 433.835-870. Smoking is prohibited within ten of any entrance or airway vent.

K. OUTSIDE EMPLOYMENT

1. District Comes First. When an individual accepts employment with the District, it is understood that the District has first call upon the services of its employees, regardless of any effect on secondary employment.

2. Incompatible Work. Employees shall not engage in outside employment that conflicts in any way with District employment, detracts from the efficiency of work performance, or is in conflict with the interests of the District. The District expects employees to avoid extra work which affects endurance, overall personal health, or effectiveness. The District will hold all employees to the same standards of performance and scheduling demands, including employees who hold outside jobs.

3. Notification. Employees shall notify the Fire Chief in writing, in advance, of all employment outside the scope of their employment with the District.

4. Conflicts. The Fire Chief will notify the employee at any time outside employment is found to be in conflict with the interests of the District or is likely to bring discredit upon the District. It shall be up to the employee to choose which employment option is most desired.

L. DRUGS AND ALCOHOL

1. Statement of Concerns.
   a. The District has a responsibility to its employees, and the public to insure safe working conditions for its employees and a productive District workforce unimpaired by chemical substance abuse. The District has a responsibility pursuant to the Drug Free Workplace Act of 1988. To satisfy these responsibilities, the District must preserve a work environment free from the effects of drugs, alcohol, or other performance-impairing substances.

   b. The misuse of alcohol and other drugs can impair employee performance, as well as physical and mental health, and may jeopardize employee safety as well as the safety of the public.

2. Policy.
   a. The District is committed to maintaining a safe and healthy work place for all employees by assisting employees to overcome drug or alcohol related problems through appropriate treatment and, if necessary, disciplinary action.

   b. Each employee is responsible for meeting performance, safety and attendance standards.

   c. Employees shall not report to work under the influence of intoxicating liquor or illegal drugs.

   d. The use, sale, possession, manufacture, distribution and/or dispensing by an employee of an intoxicating liquor, controlled or illegal substance, or a drug not medically authorized, or any other substances which impair job performance or pose a hazard to the safety and welfare of the employee, other

employees or the public, is strictly prohibited. The use of alcohol or medically prescribed controlled substances off-duty is not controlled by this policy. Conduct in violation of this policy may result in disciplinary action and/or criminal investigation, if appropriate.

e. The policy includes both voluntary and mandatory testing.

f. Employees may obtain counseling and rehabilitation through the Employee Assistance Program ("EAP").

g. Laboratory tests relied upon shall be highly accurate and reliable.

h. Positive test results may only be disclosed to the employee, the appropriate EAP administrator, the appropriate management officials necessary to process an adverse action against the employee, or a court of law or administrative tribunal in any adverse personnel action.

i. All medical and rehabilitation records in an EAP will be deemed confidential "patient" records and may not be disclosed without the prior written consent of the patient, authorizing court order, or otherwise as permitted by Federal law implemented at 42 CFR Part 2.

j. This policy will be enforced and administered in a manner which is consistent with the value statements set forth in this section, and with the advice and concurrence of the District's Board of Directors.

3. Permitted Use. It is the employees' responsibility to determine from a physician whether or not a prescribed drug can impair job performance. An employee whose impairment may affect job performance should take sick leave or other steps consistent with advice of a physician. If an employee reports to work under the influence of prescription medication and endangers self or others, the employee may be disciplined. Any failure to report the use of such drugs or other substances following an event of concern to the District, or failure to provide evidence of medical authorization, can result in disciplinary action.

4. Reports of Drug Conviction. Each employee must report facts and circumstances to the Fire Chief no later than five (5) days after conviction for violating any criminal drug statute.
   a. Employee Education. The District will afford employees an opportunity to deal with drug and alcohol related problems. The Fire District will maintain information relating to the hazards of and treatment for drug and alcohol related problems. Proactive training and information shall be sponsored by the District periodically. Any District employee may seek advice, information and assistance voluntarily. Medical confidentiality will be maintained, consistent with this policy.

   b. Employee Assistance. Any employee who voluntarily requests assistance in dealing with a personal drug and/or alcohol problem may do so through a

private treatment program for drug and alcohol problems. The Fire District will assist employees who wish to identify and select an appropriate treatment program.

If an employee seeks drug treatment voluntarily and not under adverse employment circumstances, accrued sick leave benefits may be used while attending rehabilitation. After such accommodation, the discontinuation of any involvement with alcohol or drugs may be an essential requisite for employment and is consistent with the District's policy of maintaining a drug free workplace.

5. Discipline Related to Abuse. An employee may be found to use illegal drugs on the basis of any appropriate evidence including, but not limited to:
   a. Direct observation;
   b. Evidence obtained from an arrest or criminal conviction;
   c. A verified positive test result; or
   d. An employee's voluntary admission.

   As a result of disciplinary action arising from current use of illegal drugs or job-related alcohol problem, an employee may be directed to consult with the EAP and other health care providers. Such an employee may be required to participate in a drug or alcohol treatment program as a condition of continued employment.

   A supervisor, based on reasonable suspicion that substance abuse is a factor in employment, may require an employee to be evaluated for illegal drug and alcohol use and treatment by an employee assistance program or a doctor. An employee may be required to participate in follow-up care as part of a comprehensive alcohol and drug treatment program based upon medical advice.

   When an employee is required to undergo treatment under the policy, the employee may be required to authorize the following as a condition of continued employment:
   1. Monitoring of the treatment program and the employee's participation by the District's physician; and

   2. Submission to random blood and/or urine screening for alcohol and/or drugs for a specific period of time not to exceed thirty-six (36) months.

   When an employee voluntarily enters a treatment program which is not associated with District intervention, testing and monitoring by the District will not be required.

   Medical confidentiality will be preserved, subject to rights granted by the employee to the Fire Chief to monitor treatment and program compliance through the health care provider in order to ensure compliance with conditions of employment and ability to return to or remain at work.

6. Drug Testing Upon Reasonable Suspicion. Where a supervisory employee has a reasonable suspicion that an employee is under the influence of alcohol or illegal

drugs, including unlawful use of a controlled substance without a valid prescription, the employee in question will be asked to submit to discovery testing including urinalysis or a blood screen, or both, to confirm involvement with alcohol or illegal drugs or that the employee is drug or alcohol free at the time in question.

7. Consequence of a Positive Test. An employee who is found to be under the influence of or impaired by alcohol or illegal drugs as a result of a test requested by the District based upon reasonable suspicion will be subject to disciplinary action including suspension or termination.

8. Consequence of Refusal to Submit to Testing. An employee who refuses to submit to discovery testing for alcohol and illegal drugs will be subject to suspension or discharge, or both. Alleged lack of reasonable suspicion is not grounds to refuse to submit to a test; however, it is reason to challenge discipline if discipline is imposed based on the test result alone.

9. Testing Procedure.
   a. Employee Representation. When the employee is notified that he or she is required to consent and submit to such tests, he or she may request the presence of a representative to witness the test. The test may not be delayed unreasonably in order to wait for a representative. The absence of a representative shall not be grounds for the employee to refuse to consent and submit to such tests or searches. The presence of a representative shall not disrupt or interfere with the tests or searches.

   b. Authorization to Test. Before a supervisor, acting on behalf of the District under this policy, may require an employee to consent and submit to any test, the supervisor must first obtain concurrence from the Fire Chief that the information available to the District about the subject employee is sufficient to determine reasonable suspicion that prohibited conduct will be established as a result of the test.

   c. Procedure for Consent. The employee shall give consent to a blood, urine or breathalyzer test, or any combination, upon request, by signing a consent form. The form shall contain the following information:
      I. Employee's consent to release tests results to the District;

      II. The procedure for confirming an initial positive test result for a controlled substance, including marijuana;

      III. The consequences of a confirmed positive test result for a controlled substance, including marijuana;

      IV. The consequences of a positive test for alcohol, under the circumstances;

      V. A listing provided by the employee of legally prescribed and over-the-counter medications which may be in the employee's body;

VI. The right to explain a confirmed positive test result for a controlled substance, including marijuana, or a positive test for alcohol; and

VII. The consequences of refusing to consent to the blood, urine or breathalyzer test.

i. Confirmatory Test. In the event that the blood or urine test results are positive for controlled substance(s), including marijuana, the District shall require that a second confirmatory test from the same sample be conducted, using gas chromatography/mass spectrometry methods performed by a laboratory certified by the National Institute on Drug Abuse, which also must be positive before concluding the employee has such substances(s) present in the body.

ii. Employee Requested Test. If a blood or confirmed urine test is positive, the District will instruct the laboratory to retain the blood or urine sample for a period of not less than (thirty) 30 calendar days from the date the tests are complete for the purposes of allowing the employee to conduct an independent test at his or her own expense at a laboratory approved by the District.

iii. Chain of Evidence. The procedures to obtain, handle and store blood and urine samples and to conduct laboratory tests shall be documented to establish procedural integrity and chain of evidence. Such procedures shall be administered with due regard for the employee's privacy and the need to maintain the confidentiality of tests results to an extent which is not inconsistent with the needs of this policy.

iv. Notification. The employee shall be notified of the results of all tests conducted pursuant to this policy. Employees who test positive shall be afforded an opportunity to provide medical or other information that may explain the positive test result. If a question exists, the available information will be reviewed by a licensed physician with training in forensic drug testing.

10. Pre-Employment Drug Screening. The District will invite successful applicants who are offered an opportunity to interview the opportunity to consent to a pre-employment drug screen. The applicant will be advised that the presence of one or more drugs may be cause for rejection from further consideration for employment, and that appointment to a position is contingent upon a negative drug test result. The applicant will be asked to authorize the District to conduct through the District's designated physician or laboratory testing facility a drug screen test as a requirement of employment.

Applicants shall be directed to an appropriate collection facility. The drug test must be undertaken as soon after notification as possible, and no later than 48 hours after notice to the applicant. Where appropriate, applicants may be reimbursed for reasonable travel expenses.

Applicants shall be advised of the opportunity to submit medical documentation that may support a legitimate use for a specific drug and that such information will be reviewed only by medical consultants to determine whether the individual is lawfully using an otherwise illegal drug.

The District will decline to extend a final offer of employment to any applicant with a verified positive test result, and such applicant may not reapply to the District for a period of twelve months. The Fire District shall object to the applicant on the basis of failure to pass the drug screen, a lack of personal characteristics necessary to relate to public employment or failure to support the goals of the District. The District shall inform such applicant that a confirmed presence of an illegal drug in the applicant's urine precludes the District from hiring the applicant.

11. Definitions.
    a. "Reasonable suspicion" is defined as specific articulable observations by a supervisory employee concerning the work performance, appearance (including noticeable odor of an alcoholic beverage), behavior, or speech of the employee. Any accident or incident involving physical injury to any person may be considered as constituting reasonable suspicion for discovery testing for drugs and alcohol where human factors contribute to the incident and a question of sobriety short of reasonable suspicion exists.

       Reasonable suspicion testing may be based upon, among other things:
       I. Observable phenomena, such as direct observation of drug use or possession and/or the physical symptoms of being under the influence of a drug;

       II. A pattern of abnormal conduct or erratic behavior;

       III. Arrest or conviction for a drug related offense, or the identification of an employee as the focus of a criminal investigation into illegal drug possession, use, or trafficking;

       IV. Information provided either by reliable and credible sources or independently corroborated; and

       V. Newly discovered evidence that the employee has tampered with a previous drug test.

       Although reasonable suspicion testing does not require certainty, mere "hunches" are not sufficient to meet this standard.

    b. "Under the influence" is defined as any detectable level of a controlled substance (in excess of trace amounts attributable to secondary exposure) in an employee's blood or urine or any noticeable or perceptible impairment of

the employee's mental or physical faculties. With respect to alcohol, a blood alcohol content of .004% constitutes under the influence while on duty.

c. "Controlled substances" are defined as all forms of narcotics, depressants, stimulants, hallucinogens, cannabis, and other controlled substances of which the sale, purchase, transfer, use or possession is prohibited or restricted by The Federal Controlled Substances Act. "Illegal or controlled substances" means a controlled substance included in Schedule I or II, as defined by section 802(6) of Title 21 of the United States Code, the possession of which is unlawful under chapter 13 of that Title. The term "illegal drugs" does not mean the use of a controlled substance pursuant to a valid prescription or other uses authorized by law.

d. "Over-the-counter drugs" are those which are generally available without a prescription from a medical doctor and are limited to those drugs which are capable of impairing the judgment of an employee to safely perform his or her duties.

e. "Prescription drugs" are defined as those drugs which are used in the course of medical treatment and have been prescribed and authorized for use by a licensed practitioner/physician or dentist.

f. Searches. Employees have no expectation to be free from search of a locker, desk or contents of other similar District controlled spaces. A search for contraband within personally controlled spaces on District property (purses, garments, brief cases or a personal vehicle, for example) shall be based on reasonable grounds or consent of the employee. In accordance with the provisions of this policy prohibiting drugs in the work place, or based upon legitimate concerns for the possession of other unauthorized materials (such as firearms, explosives or stolen property,) this policy constitutes formal notice of the District's intent to search premises, persons and secured spaces, including vehicles parked on District property, based upon reasonable grounds or consent. Searches shall be approved by the Fire Chief or his/her designee, and, if possible, notice to the employee and an opportunity to be present shall be given.

g. Refusal. Failure to appear for testing without a deferral will be considered refusal to participate in testing, and will subject an employee to the range of disciplinary actions, including dismissal, and an applicant to the cancellation of an offer of employment. If an individual fails to appear at the collection site at the assigned time, the collector shall contact the Fire Chief to obtain guidance on action to be taken.

M. CREDIT CARD USE

This policy will apply to all District personnel using District credit cards. The Districts policy is to ensure prudent use of public monies entrusted to the District for operations. Personnel using these cards must turn in itemized receipts for each charge. The receipt must clearly show the item(s) purchased, date, and store where

purchased. Documentation on each receipt is to include the person making the purchase, what the items are for, and for which station, when applicable. Lost or stolen credit cards must be reported immediately to the credit card company to minimize risk to the District. The Fire Chief will also be notified. Itemized food receipts must be provided when using a District credit card for meals. Personnel possessing a District credit card may be held accountable for any charges on the credit card statement if an itemized receipt is not provided.

N. IDENTITY THEFT PREVENTION PROGRAM

1. Purpose

This policy is intended to establish an Identity Theft Prevention Program ("the Program"). The Program is designed to detect, prevent and mitigate Identity Theft in connection with certain District accounts, programs, or procedures (including specifically utility accounts). This policy applies to District accounts, programs, or procedures which allow a person or an entity to make multiple payments on personal, family, or household accounts and presents a "reasonably foreseeable risk" of Identity Theft. As general guidance, this policy will apply to any District account, program, or procedure which allows multiple household or personal payments and collects, transfers, stores, or records a person's personally identifiable information. This policy complies with Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act) of 2003 and, by law, is deemed in compliance with the Oregon Identity Theft Act as provided by ORS 646A.622(2)(a) and (b). After consideration of the size and complexity of the District's operations and the nature and scope of the District's activities, the District's governing body has determined that the Program is appropriate for the District and has approved the Program on January 21, 2010.

2. Definitions

A covered account means:

a. An account the District offers or maintains primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts may include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, *utility accounts*, checking accounts and savings accounts; and

b. Any other account the District offers or maintains for which there is a reasonably foreseeable risk of Identity Theft to customers or a risk to the safety and soundness of the District's utility of Identity Theft, including financial, operational, compliance, reputation or litigation risks.

Identify theft means fraud committed or attempted using the Identifying Information of another person without authority.

A Red Flag means a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Identifying Information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, Social Security number, date of birth, government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or unique electronic identification number.

Security Information is defined as government data the disclosure of which would be likely to substantially jeopardize the security of Identifying Information.

3. Program

The District hereby establishes an Identity Theft Prevention Program to detect, prevent and mitigate Identity Theft. The Program includes procedures to:

a. Identify Red Flags for covered accounts and incorporate those Red Flags into the Program;

b. Detect Red Flags that have been incorporated into the Program;

c. Respond appropriately to any detected Red Flags to prevent and mitigate Identity Theft; and

d. Update the Program periodically to reflect changes in risks to customers and to ensure the safety and soundness of the utility from Identity Theft.

4. Program Administration
   Oversight
   Responsibility for developing, implementing and updating this Program lies with the Fire Chief.
   The Fire Chief will be responsible for:
   a. Program resources and planning;

   b. Ensuring appropriate Program training of utility staff;

   c. Reviewing any staff reports regarding Red Flag detection and Identification Theft mitigation and prevention;

   d. Determining which steps of prevention and mitigation should be taken in particular circumstances commensurate with the risk posed; and

   e. Considering periodic changes to the Program.

5. Staff Training and Reports
   Staff responsible for implementing the Program will be trained by or under the direction of the Program Administrator. Staff will provide timely reports to the Program Administrator on all incidents of Identity Theft or occurrences of Red Flags.

6. Program Review and Updates
   The Fire Chief will review and update this Program at least once a year to reflect changes in risks to customers and the soundness of District programs from Identity Theft. In doing so, the Program Administrator will consider the District's experience with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the District's business arrangements with other entities. After considering these factors, including the degree of Identity Theft risk posed, the Program Administrator will determine whether changes to the Program, including the listing of new Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the District's governing body with recommended changes and the governing body will make a determination of whether to accept, modify or reject those changes to the Program.

7. Identification of Red Flags
   In order to identify Red Flags, the District considers the types of accounts or programs it offers and maintains, the methods it uses to open and access accounts, and its previous experiences with Identity Theft. The District has identified the following Red Flags in each of the listed categories:

8. Notifications and Warnings from Credit Reporting Agencies
   Red Flags
   a. Report of fraud accompanying a credit report;

   b. Notice or report from a credit agency of a credit freeze on a customer

or applicant;

c. Notice or report from a credit agency of an active duty alert for an applicant; and

d. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

9. Suspicious Documents
Red Flags
   a. Identifying Information that appears to be forged, altered or inauthentic;

   b. Identifying Information on which a person's photograph or physical description is inconsistent with the person presenting the document;

   c. Other document with information that is inconsistent with existing customer information (such as if a person's signature on a check appears forged); and

   d. Application that appears to have been altered or forged.

10. Suspicious Personal Identifying Information
Red Flags
   a. Identifying Information presented inconsistent with other information the customer provides (example: inconsistent birth dates);

   b. Identifying Information presented inconsistent with other sources of information (for instance, an address not matching an address on a credit report);

   c. Identifying Information presented that is the same as information shown on other applications that were found to be fraudulent;

   d. Identifying Information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

   e. Social security number presented that is the same as one given by another customer;

   f. An address or phone number presented that is the same as that of another person;

   g. Failure to provide complete personal Identifying Information on an application when reminded to do so (however, Social Security numbers must not be required); and

h. Identifying Information inconsistent with the information on file for the customer.

11. Suspicious Account Activity or Unusual Use of Account
Red Flags
a. Change of address for an account followed by a request to change the account holder's name;

b. Payments stop on an otherwise consistently up-to-date account;

c. Account used in a way inconsistent with prior use (example: very high activity);

d. Mail sent to the account holder is repeatedly returned as undeliverable;

e. Notice to the District that a customer is not receiving mail sent by the District;

f. Notice to the District that an account has unauthorized activity;

g. Breach in the District computer system security; and

h. Unauthorized access to or use of customer account information.

12. Alerts from Others
Red Flag
Notice to the District from a customer, Identity Theft victim, law enforcement or other person that the District has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

13. Detecting Red Flags
New Accounts
In order to detect any of the Red Flags identified above associated with the opening of a new account or program which pertains to household or personal matters (such as a utility account) or which presents a foreseeable risk of Identity Theft, District personnel will take the following steps to obtain and verify the identity of the person or business opening the account:

a. Require certain Identifying Information, which may include:
I. Full name;
II. Date of birth (for individual);
III. Previous and current residential or business address;
IV. Principal place of business (for an entity); and
V. Identification. Required identification may include the following:

I. For a U.S. Citizen
1. Taxpayer Identification number (for business) or Social

Security number; and/or

2. Photo-bearing documents (original required) such as:
   A. State-issued driver's license; or
   B. State-issued identification card; or
   C. Passport from any country

II. For a Non-U.S. Citizen
   1. Social Security number; and/or
   2. Photo-bearing documents (original required) such as:
      A. State-issued driver's license; or
      B. State-issued identification card; or
      C. Passport from any country; or
      D. Documents containing an alien identification number and country of issuance; or
      E. Any other photo-bearing government-issued document evidencing nationality or residence.

b. Review all documentation for Red Flags; and/or independently contact the customer.

14. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account or program**, personnel will take the below steps to monitor transactions with an account. District personnel have the discretion to determine the degree of risk posed and to act accordingly.

a. Verify customer's Identifying Information if a customer requests any information on the account (this can be done in person, via telephone, via facsimile, or via email);

b. Verify the validity of requests to change billing addresses; and

c. Verify changes in banking information given for payment purposes.

15. Preventing and Mitigating Identity Theft

a. **Ongoing Operations to Prevent Identity Theft.** In order to further prevent the likelihood of Identity Theft, personnel will take the below steps, commensurate with the degree of risk posed, regarding ongoing internal operating procedures. District personnel have the discretion to determine the degree of risk posed and to act accordingly.

   I. Ensure that its website is secure or provide clear notice that the website is not secure;

   II. Ensure complete and secure destruction of paper documents and computer files containing customer Identifying Information;

   III. Ensure that office computers are password protected;

IV. Keep offices clear of papers containing customer information;

V. Ensure computer virus protection is up-to-date;

VI. Review District processes and require and keep only information necessary for program purposes;

VII. Transmit Identifying Information using only approved methods and include the following statement on any transmitted Identifying Information:

> *"This message may contain confidential and/or proprietary information, and is intended for the person/entity to which it was originally addressed. If you have received this email by error, please contact the District and then shred the original document. Any use by others is strictly prohibited."*

VIII. Does not use or post customer's Social Security number as an account identifier or on any other documents unless requested by customer or required by federal law (such as W-2 forms).

b. **Steps to take when you Detect a Red Flag.** In the event District personnel detect Red Flags, they will take *one or more* of the below steps, commensurate with the degree of risk posed, to prevent and mitigate risk of Identity Theft. District personnel have the discretion to determine the degree of risk posed and to act accordingly.

I. Continue to monitor an account for evidence of Identity Theft;

II. Contact the customer either by written notice or telephone;

III. Refuse to open a new account;

IV. Close an existing account;

V. Reopen an account with a new number;

VI. Notify the Program Administrator for determination of the appropriate step(s) to take;

VII. Notify law enforcement; or

VIII. Determine that no response is warranted under the particular circumstances.

c. **Steps to take when you receive notice of an address discrepancy.**
In the event the District receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report, the District will reasonably confirm that an address is accurate by any of the following means:

I. Verify the address with the consumer;

II. Review District records;

III. Verify the address through third-party sources; or

IV. Use other reasonable means to verify the address.
If an accurate address is confirmed, the District will furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice if:

i. The District establishes a continuing relationship with the consumer; **and**

ii. The District, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.

16. Service Provider Arrangements
In the event the District engages a service provider to perform an activity in connection with a Covered Account, the District will take one of the following steps to ensure the service provider performs in accordance with the Program:

a. Require, by contract, that service providers have appropriate policies and procedures in place designed to detect, prevent, and mitigate Identity Theft; or

b. Require, by contract, that service providers review this Program and report any Red Flags to the Program Administrator; and

c. The above specified contracts shall include indemnification provisions limiting the District's liability for the service provider's failure to detect, prevent, or mitigate Identity Theft.

17. Non-disclosure of Specific Practices
Disclosure of specific information or practices regarding Red Flag identification, detection, mitigation and prevention practices may be limited to designated District staff and/or policymakers. Documents produced to develop or implement the Program which describe specific practices may constitute Security Information and may be non-disclosable because disclosure would likely jeopardize the security of Identifying Information and may circumvent the District's Identity Theft prevention efforts.