Protection of Social Security Numbers and Other Personal Information

Effective October 1, 2008

Connecticut Water Service, Inc. and The Connecticut Water Company ("Companies") are aware of the significant risks of identity theft and the potential impact to our customers, vendors, employees, shareholders of such activity. The Company is not aware of any incidents or complaints of identity theft associated with our accounts, but recognize we have a responsibility as a business to take measures to identify potential risks and determine procedures to prevent and mitigate identity theft.

This Identity Theft Prevention Program ("Program") has been developed to meet that responsibility and to satisfy the requirements of state and federal laws, including the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 and Connecticut PA 08-167 regarding protection of Social Security numbers. The Company has in place other policies and programs, such as the IT security policies or Sarbanes Oxley Controls, that may support these efforts. Those policies remain in effect and are not intended to be superseded by this policy.

EXPECTATIONS OF EMPLOYEE CONDUCT

Connecticut Water Service, Inc. has reflected in its Employee Code of Conduct for the Companies the fundamental principals for how we conduct business and the expectations of our employees in the performance of their duties. Those principals and practices support the underlying objectives of the Rule by promoting business practices that protect our customers, shareholders and employees interests and confidential information. The following provisions of the Code of Conduct pertaining to Our Principal and Business Practices are incorporated in the Program for Identity Theft Protection.

> *Ethical conduct is fundamental to good business. The nature of our business imposes special obligations of public trust upon us. We are committed to meeting those obligations without compromise. Accordingly, the highest standards of ethical conduct, regulatory compliance, and legal behavior govern our actions. Business will be conducted with our best skills and judgment for the benefit of shareholders, customers, employees, and the environment.*

Further, the Code of Conduct ensures employees are aware of and accept responsibility to protect confidential information from disclosure or abuse as follows:

> *Confidential Information – Company information, including among other things, financial data, mergers/acquisitions, business processes and procedures, computer programs, wage and salary information, customer/supplier/subcontractor and other information and developments not released to the general public, must be used solely for Company purposes and never for personal gain. Confidential information must not be shared with anyone outside of the Company unless they have a legitimate need to know in order to do business with us. Employees who have access to Company confidential information must protect that information from disclosure. Additionally, employees who have access to confidential information shall not reveal the source or content of such information to individuals within the company, except as necessary for business purposes.*

PROTECTING INFORMATION, PREVENTING AND MITIGATING IDENTITY THEFT

Identifying or confidential information

The Company will collect, retain and use identifying or confidential information only when we believe it is reasonably necessary or useful for us to operate the utility or an affiliated company. We may disclose nonpublic personal information for business purposes to an affiliated company or nonaffiliated organizations such as service providers or other companies that process payments or other transactions, or assist us with mailings or other business functions. We reserve the right to disclose all of the information we collect to these companies and organizations. We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law such as when requested or consented to by the consumer; to conduct business; or to law enforcement and regulatory authorities.

In order to prevent the likelihood of identity theft occurring with respect to such information, the Company will take the following steps with respect to its internal operating procedures to protect identifying or other confidential information:

Protecting identifying or other confidential information

1. Require and keep only the kinds of information for customers, employees, vendors or registered shareholders that are necessary for the company's purposes.
2. Ensure that paper documents that contain confidential information are stored in locked cabinets and secured when not in use;
3. Keep offices clear of documents containing protected personal and/or confidential information;
4. Provide for electronic scanning and storage of documents that have confidential information. Limit access to confidential electronic files such that they are used only as required for legitimate business or legal purposes and are protected by password;
5. Ensure complete and secure destruction of paper documents and computer files containing customer information;
6. Ensure that office computers are password protected and that computer screens lock after a set period of time;
7. Implement internal controls to monitor access to electronic records;
8. Ensure computer virus protection is up to date; and
9. Ensure that its website is secure or provide clear notice that the website is not secure.