IDENTITY THEFT

Section 1. PURPOSE

A. The Federal Trade Commission ("FTC") instituted a rule that became effective November 1, 2008 ("Rule"), whereby all creditors, as defined in the Rule, must implement a written identity theft prevention program to detect, prevent, and mitigate identity theft in connection with the opening of an account or any existing account. The Bedford Regional Water Authority ("Authority") is a creditor for purposes of the Rule.

B. The Authority shall take certain steps to comply with the Rule of the program as hereinafter defined, which shall then constitute the Authority's Identity Theft policy. Also contained in this policy are the Authority procedures for compliance with the Virginia breach of personal information notification statute.

Section 2. NEW CUSTOMER ACCOUNTS

A. Whenever any new customer applies to the Authority for water and/or sewer service, the Authority shall require the applicant to submit certain information, including but not limited to, the applicant's name, the address for which service is requested, and the applicant's social security number or federal tax identification number ("TIN")

B. Upon the securing of this information, the Authority shall run a check on these three (3) information fields against the Authority's current database in order to see if any of the fields are duplicates.

C. In the event that any duplicate names, addresses, social security numbers, or TIN show up on the Authority's current database, the Authority shall identify the duplicates as "Red Flags" and shall then use due diligence in order to determine whether any identify theft is being attempted or has occurred.

D. Such due diligence shall include an attempt to verify the validity of any new customer information that is submitted and that has been identified as a Red Flag, as well as an attempt to verify the validity of the information on the existing database that comprises the Red Flag. If, in the Authority's opinion, invalid information has been submitted or exists on the system, the Authority shall notify the customer(s) in question. As appropriate, the Authority may also take other steps including the following:
   1. Monitoring of the new and existing accounts.
   2. Reopening accounts with new account numbers.
   3. Not opening the new account.
   4. Closing the existing account.
   5. Not attempting to collect on accounts or not selling accounts to debt collectors.
   6. Notifying law enforcement officials.
   7. Making a determination that no response is warranted under the particular circumstances.

Section 3. EXISTING CUSTOMER ACCOUNTS

The Authority shall regularly monitor existing customer accounts, authenticating customers where necessary, monitoring transactions and any suspicious account activity, and verifying the validity of any change of address requests or other account change requests. In addition, where appropriate, the Authority may also take any of the steps listed in Section 2.D as stated above.

Section 4. ONGOING ADMINISTRATION

The Authority shall take such steps so as to periodically update its procedures for detecting Red Flags and potential identity theft, taking into account factors such as the Authority's experiences with identity theft and changes in the methods to identify and mitigate identity theft. As well, the Authority's Board of Directors or one of the assigned Committees shall have oversight over this policy and shall be provided reports by Authority staff generated in conjunction with the running of this policy. In addition, the Authority shall update this policy from time to time as needed, and in order to maintain compliance with the Rule, as contained in 16 CFR Part 681.

Section 5. VIRGINIA BREACH OF PERSONAL INFORMATION NOTIFICATION STATUTE

A. The Authority shall take such steps as are necessary in order to stay in compliance with the Virginia Breach of Personal Information Notification Statute, Virginia Code Section 18.2-186.6 ("Statute"). The Statute requires the Authority to report any unauthorized breaches of its customer database or other systems housing personal information of its customers. The report must be made to both the Office of the Attorney General and to any affected customer whose personal information has been, or is reasonably believed to have been, accessed and acquired by an unauthorized person. The Statute specifies the type of notice that is acceptable. Acceptable notice includes the following:
   1. Written notice to the last known postal address in the records of the customer or business.
   2. Telephone notice.
   3. Electronic notice.
   4. Substitute notice, in specific instances under the Statute.

B. The contents and description to be included in the notice are specified in the Statute. The Authority shall update this policy from time to time in order to maintain compliance with the Statute.

Section 6. REVISIONS

A. This policy was approved and adopted by the Authority's Board of Directors on March 26, 2013, effective July 1, 2013.