HUNTSVILLE UTILITIES POLICY

Revision Approval Date: **Gas & Waterworks Board-9/19/2019** **Electric Board- 9/25/2019**	**Date Posted: 9/27/2019**	**Implementation Date: 10/1/2019**

Policy #: **CC-02**

Policy: **Identity Theft Prevention**

Purpose: To establish an Identity Theft Prevention Program (Program) that will reduce the risk of identity theft and fraud and maintain compliance with the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

Overview:

Huntsville Utilities (HU) is subject to administrative enforcement of the FACT Act by the Federal Trade Commission (FTC). The FTC requires development and implementation of a written program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or maintaining any existing covered account. HU will determine the scope of our program by conducting a risk assessment of how customer accounts are opened, how customers are provided access to their accounts, and our previous experiences with identity theft.

Administration of the Program:

1. Privacy Committee - The Senior Vice President of Customer Care shall establish a Privacy Committee (Committee), and appoint the Customer Services Manager (CSM) to serve as the Privacy Officer and chair the Committee. The Privacy Officer will coordinate Committee meetings, prepare an annual report for Executive Management, respond to audits, and any other activities to assure compliance with this policy. Additional members of the committee shall be chosen by the head of the representative departments and will at a minimum include representatives from Customer Relations, Information Technology, and Human Resources.

   The Committee will conduct an annual risk assessment. Results of the risk assessment will aid in development or update of written operations standards and procedures that incorporate processes to ensure compliance with the FACT Act, including:

   a. Annual training of applicable employees.
   b. Identifying and documenting relevant red flags of identity theft that may occur in our day-to-day operations. Red Flags are suspicious patterns, practices, or specific activities that indicate the possibility of identity theft.
   c. Detecting when the identified red flags exist.
   d. Responding appropriately to any red flags that are detected.
   e. Creating documentation of suspected identity theft activity.
   f. Retaining documentation in compliance with established HU Record Retention Policies, Standards, and Procedures.
   g. Updating the Program periodically to reflect changes in risks to customers and HU.

   The Committee convenes as needed, a minimum of once annually, to review and update the existing standards and procedures, study suspected and confirmed identity theft activity to determine changes in risks, and approve the report that will be presented to members of Executive Management and/or the CEO. The report should include an evaluation of the effectiveness of the standards and procedures, significant incidents involving identity theft and management's response, and recommendations for material changes to the program.

2. Management – It is the responsibility of HU management to ensure compliance with this policy by providing the policy to their applicable employees and scheduling them for annual training. Each manager is responsible for immediately reporting suspected incidents of identity theft to the Privacy Officer.

3. Employees - All employees of HU, including part-time and temporary personnel, are responsible for adherence to this policy. Applicable employees must attend annual training as scheduled by their manager. Employees should immediately report suspected incidents of identity theft to their supervisor.

4. Third Parties – Requirements for third parties (vendors, consultants, contractors, or others with service agreements) utilized by HU are documented in financial management, information technology, and governance policies, standards, and procedures.

Related Policies, Standards, and Procedures:

- IT-01 Information Management & Security Policy
- IT-02 Customer Data Privacy Policy
- OS-IT-001 Security Awareness Training Operational Standard
- 002-2016 Computer System Use & Security Operational Policy (procedure)
- 003-2016 Use and Protection of Data Operational Policy (procedure)

Original Issue Date: 10/25/08

Revision Dates: 3/14, 3/15, 10/1/21 (N/C)