NEW BRAUNFELS UTILITIES

MEMORANDUM

To: **NBU Audit Committee of the Board of Trustees**

From: **Greg Brown, Chief Technology and Security Officer**

Date: **December 3, 2024**

Subject: **Red Flag Report for 2024**

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) required reasonable procedures to identify “Red Flags,” defined by the Federal Trade Commission as "a pattern, practice, or specific activity that indicates the possible existence of identity theft." In response to the FACTA of 2003, New Braunfels Utilities (NBU) has adopted the Identity Theft Prevention Policy to mitigate potential threats via proactive measures and reporting. NBU implemented the Identity Theft Prevention Program to manage the following activities for “Red Flag” identification:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the program;
2. Incorporate Red Flags already identified in existing NBU Policy into the program;
3. Describe and establish appropriate responses to any Red Flags as detected to prevent and mitigate identity theft and
4. Update the Program periodically to assess changes in customer risk incidents, risk identification or classification methods, supervisory oversight requirements, and training needs.

Incidents:

For the 2024 calendar year, there have been no red-flag incidents.

Accomplishments

In 2024, the Cybersecurity Team successfully launched a comprehensive Vulnerability Management Program and enhanced the Security Information and Event Management (SIEM) platform. These initiatives significantly strengthened the organization’s in-depth defenses against cyber threats. The Vulnerability Management Program helps identify and address security weaknesses in the enterprise systems. The SIEM program continuously monitors the network for suspicious activities and potential security breaches. The SIEM provides proactive responses to possible threats in a rapid and effective manner. These programs are two additional elements in a cybersecurity portfolio that protect classified and sensitive data and ensure regulatory compliance.

In 2024, the Physical Security Team successfully implemented several critical security initiatives. A new Key Management System is in the process of being deployed. The system ensures that only authorized personnel have access to sensitive areas. A new Visitor Management System is also in the process of being deployed at the Customer Solution Center. This system will track and monitor all visitors in the facility, ensuring an awareness of persons in our facilities at all times. Additionally, the installation of a fail-safe button on all magnetically locked doors at the Service Center is complete. The button ensures the doors will be opened during outages that affect the magnetic locks. Finally, a comprehensive security evaluation of all NBU sites has been completed. The evaluation will result in a gap analysis and prioritization of projects to strengthen our security posture.

Per Texas House Bill 3834, our Cybersecurity and Learning & Development teams provided the following training required by the State of Texas:

Texas Cybersecurity Awareness Training 2024

- Topic Included:
  - Information Security Habits
  - Procedures that protect Information Resources
  - Best practices for detecting, assessing, reporting, and addressing Information Security Risks

A total of 437 employees completed the training by July 2024, a 100% completion rate.

In Summary:

The existing Identity Theft, Red Flag, and Suspicious Activity detection methods, as described in the NBU Identity Theft Prevention Policy, remain reasonable, appropriate, and sufficient to mitigate risks to NBU and its customers.

Per Texas House Bill 3834, cybersecurity training and proof of compliance will be required annually. All NBU employees will be required to complete the training. The Cybersecurity and Learning & Development teams will continue implementing and deploying the training program.