Exhibit to Agenda Item #1

Strategic Direction SD-16, Information Management and Security.

Board Policy Committee and Special SMUD Board of Directors Meeting

Wednesday, November 15, 2023, scheduled to begin at 6:00 p.m.

Powering forward.
Together.

SMUD®

SD-16 Information Management and Security Policy

Proper management of cyber and physical information, as well as physical security, is a core value. Robust information management and physical security practices are critical to effective risk management and to ensure regulatory compliance, business resiliency and customer satisfaction. SMUD shall take prudent and reasonable measures to accomplish the following:

a) Information Security: SMUD will protect customer, employee and third-party information, and SMUD information systems are protected from unauthorized access, use, disclosure, disruption, modification, or destruction.

b) Physical Security: SMUD will safeguard its employees while at work as well as customers and visitors at SMUD facilities. SMUD will also protect its facilities and functions that support the reliability of the electric system and overall operation of the organization from unauthorized access or disruption of business operations.

c) Customer Privacy: SMUD will annually notify customers about the collection, use and dissemination of sensitive and confidential customer information. Except as provided by law or for a business purpose, SMUD will not disseminate sensitive and confidential customer information to a third party for non-SMUD business purposes unless the customer first consents to the release of the information. Where sensitive and confidential information is disseminated for a business purpose, SMUD will ensure: (i) the third party has robust information practices to protect the sensitive and confidential customer information, and (ii) use of the information by the third party is limited to SMUD's business purpose. SMUD will maintain a process that identifies the business purposes for which SMUD will collect, use and disseminate sensitive and confidential customer information.

d) Records Management: SMUD will maintain the efficient and systematic control of the creation, capture, identification, receipt, maintenance, use, disposition, and destruction of SMUD records, in accordance with legal requirements and Board policies.

Monitoring Summary

SMUD is in substantial compliance with SD-16, Information Management and Security Policy.

2023 Activities

- Information Security
  - Program aligned to National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Customer Privacy
  - Annual notice of privacy practices sent with May bill cycle
  - No data shared for non-SMUD business purposes
  - Data Security where data is shared
    - Data Sharing Audit – all observations closed (Nov 2022)
    - Supply Chain Risk Management and Vendor Security Requirements
    - Cybersecurity Emergency Operations Program (CEOP)

2023 Activities

- Payment Card Industry (PCI) - Data Security Standard (DSS)
- SMUD is Compliant
- Version 4 transition period started (until 31 March 2024)
- Merchant Bank: Chase Paymentech
- Level 2 Merchant – transaction volumes (for 2022 full calendar year):
  - Visa: 1,923,941
  - MasterCard: 454,602
  - AmEx: 10,897
  - Discover: 36,135
- PCI DSS Self-Attestation required Annually
  - Self-Assessment Questionnaires (SAQ) submitted to Merchant Bank 14 June 2023

2023 Activities

- Physical Security
  - Training on new radio communications link with local law enforcement
    - Facilitates direct communication during critical incidents
  - Began replacement of the Physical Access Control System
    - System procured
    - Project underway
  - Third-party Risk, Threat, and Vulnerability Analysis (RTVA) project
    - Independent evaluation
    - Will allow for identification and mitigation of security-centric issues

2023 Activities

- Information Management & Compliance
  - Completed the 5-year record evaluations plan
    - Implemented Information Management Procedures
  - Launched mass content migration (Enterprise Shared Drive Migration) project
    - Kicked off for 13 of the 33 business areas in scope
    - From non-approved to approved record repositories
  - Partnered with IT to review software integrations
    - Added IMC review to purchase approval process
  - Continued collaboration with IT and governance groups within SMUD
    - Enterprise Content Management Team, Cybersecurity, the Critical Infrastructure Protection (CIP) Program, Data Governance and others

Questions and Answers