

# Exhibit to Agenda Item #1

Accept the monitoring report for **Strategic Direction SD-16, Information Management and Security.**

Board Policy Committee and Special SMUD Board of Directors Meeting  
Wednesday, November 16, 2022, scheduled to begin at 5:30 p.m.  
Virtual Meeting (online)

# 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.

# 2022 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, improvements to Policy and Process
    - Supply Chain Risk Management and Vendor Security Requirements
    - Cybersecurity Emergency Operations Program (CEOP)

# 2022 Activities

- Payment Card Industry (PCI) - Data Security Standard (DSS)
- SMUD is Compliant
- Version 4 approved, transition period until 31 March 2024
- Merchant Bank: Chase Paymentech
- Level 2 Merchant – 2021 transaction volumes:
  - Visa: 1,681,492
  - MasterCard: 371,944
  - AmEx: 9,336
  - Discover: 30,261
- PCI DSS Self-Attestation required Annually
  - Self-Assessment Questionnaires (SAQ) submitted to Merchant Bank 10 June 2022
  - Cybersecurity completed required Self-Assessment Questionnaires 2 June 2022

# 2022 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
  - Computer-Aided Dispatch and Records Management System (CAD/RMS)
    - Project Underway
    - Will allow for upgraded metrics collection and operational efficiency

# 2022 Activities

- Records & Information Management (RIM)
  - Continued completing record evaluations (in year 4 of 5-year plan)
    - Projecting completion by YE 2023
    - Continuing to streamline processes
  - Collaboration with Enterprise Content Management (ECM) to launch mass content migration project in 2023
    - From non-approved to approved record repositories
  - Partnered with IT to review software integrations
    - Adding RIM review to purchase approval process
  - Continued collaboration with IT and governance groups within SMUD
    - Microsoft 365 Governance Oversight team, the Critical Infrastructure Protection (CIP) Program and others

# Questions and Answers