Exhibit to Agenda Item #1

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

Board Policy Committee and Special SMUD Board of Directors Meeting

Wednesday, November 12, 2025 scheduled to begin at 6:00 p.m.

SMUD Headquarters Building, Auditorium

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) **Cybersecurity**: SMUD will protect customer, employee and third-party information, and SMUD technology 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 or employee 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 and employee information.

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

Monitoring Summary

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

2024-2025 Activities

- Cybersecurity
  - Program aligned to National Institute of Standards & Technology (NIST)
  - Zero Trust Strategy
  - Enhanced Third Party Risk Management

- Customer Privacy
  - Annual notice of privacy practices sent with May bill cycle
  - No data shared for non-SMUD business purposes
  - Data Sharing policy and process remain effective

2024-2025 Activities

- Payment Card Industry (PCI)
  - Data Security Standard (DSS)
- SMUD is compliant with PCI standard
- Merchant Bank: Chase Paymentech
- Level 2 Merchant – transaction volumes (for 2024 full calendar year):
  - Visa: 2,262,461
  - MasterCard: 483,436
  - AmEx: 13,433
  - Discover: 40,215
- PCI DSS Self-Attestation required Annually
  - Self-Assessment Questionnaires (SAQ) submitted to Merchant Bank June 13, 2025

2024-2025 Activities

- Physical Security
  - Approval of Off-Cycle Budget Request of $2M per year for 2026 & 2027 Budget for Upper American River Project Technology Upgrades
  - Computer Aided Dispatch System
  - Risk, Threat, Vulnerability Assessment of SMUD Facilities
  - Continued Partnership with Volunteers of America
  - Situational Awareness Training for Field Crews
  - Continued Landscape Hardening at Substations
  - Design Incorporation of Substation Security Standards
  - Letter of Agency Agreements with Sacramento Sheriff & Sacramento PD
  - 2025 NERC Audit – No Findings
  - “See Something, Say Something” & “Power of Hello” Campaigns
  - Customer Service Center Lobby Counter Improvements

2024-2025 Activities

- Information Management & Compliance
  - Enterprise Content Migration Project
    - Planned completion of 40 out of 40 total business areas by year end
    - Estimated total of 7 million documents classified & migrated
    - Implemented comprehensive Information Management procedures for all migrated areas
  - Data Loss Prevention (DLP) Program
    - Governance model to classify & protect sensitive information
    - Safeguards sensitive information & reduces risk of data breach
    - Planned enterprise implementation in 2026
  - Continued collaboration with IT and governance groups within SMUD
    - Enterprise Content Management Team, Cybersecurity, Data Governance, the Critical Infrastructure Protection (CIP) Program and other

Questions and Answers