

Exhibit to Agenda Item #2

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

Board Energy Resources & Customer Services Committee and Special SMUD Board of Directors Meeting

Wednesday, December 9, 2020, 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.

2020 Activities

- Information Security
 - Program aligned to National Institute of Standards and Technology (NIST) Cybersecurity Framework (shared in closed session)
- Customer Privacy
 - Annual notice of privacy practices sent with June bill cycle
 - No data shared for non-SMUD business purposes
 - Data Security where data is shared
 - Data Sharing Policy and Request Form
 - Supply Chain Risk Management and Vendor Security Requirements
 - Incident Response Plan
 - California Consumer Privacy Act (CCPA)

2020 Activities

- Payment Card Industry (PCI) - Data Security Standard (DSS)
- SMUD is Compliant
- Merchant Bank: Chase Paymentech
- Level 2 Merchant – 2019 transaction volumes:
 - Visa: 1,722,046
 - MasterCard: 286,380
 - AmEx: 8,687
 - Discover: 24,202
- PCI DSS Self-Attestation required Annually
 - Treasury attest required Self-Assessment Questionnaire(s) 18 September 2020
 - Cybersecurity completed required Self-Assessment Questionnaire(s) (SAQ) 21 September 2020

2020 Activities

- Physical Security
 - Improved communication system with local law enforcement agencies
 - Risk assessment performed for the Physical Access Control System
 - Third party Risk, Threat, and Vulnerability Analysis (RTVA) planned
 - Ongoing evaluations of substation physical security by Officers on patrol
 - Continued efforts to limit unauthorized physical access
 - Ongoing on the job training performed by senior Officers

2020 Activities

- Records Management
 - Continued record evaluations (in year 2 of 5-year plan)
 - COVID impacted
 - eCommunications policy rolling out, addressing retention of:
 - Chats & Recordings (2020)
 - Email (2021)
 - Partnered with IT to review software integrations
 - Example: Office 365/SharePoint Online, Teams, Outlook
 - Onboarded software tool for disposing of records across multiple platforms
 - Audit & Quality Services' audit 28006022 Records Management (2014) finding #02 addressed

Questions and Answers