



Moody/Brown

RESOLUTION NO. 6526

WHEREAS, the Board of Directors has determined it is in the best interest of the District, its employees, and its customer-owners to establish written policies that describe and document OPPD's corporate governance principles and procedures; and

WHEREAS, each policy was evaluated and assigned to the appropriate Board Committee for oversight of the monitoring process; and

WHEREAS, the Board's Governance Committee (the "Committee") is responsible for evaluating Board Policy SD-12: Information Management and Security on an annual basis. The Committee has reviewed the 2022 SD-12: Information Management and Security Monitoring Report and finds OPPD is taking reasonable and appropriate measures to comply with Board Policy SD-12 as stated.

NOW, THEREFORE, BE IT RESOLVED that the Board of Directors of Omaha Public Power District accepts the 2022 SD-12: Information Management and Security Monitoring Report, in the form as set forth on Exhibit A attached hereto and made a part hereof, and finds that OPPD is taking reasonable and appropriate measures to comply with Board Policy SD-12: Information Management and Security.



Board Action

BOARD OF DIRECTORS

October 18, 2022

ITEM

SD-12: Information Management and Security Monitoring Report

PURPOSE

To ensure full board review, discussion and acceptance of SD-12: Information Management and Security Monitoring Report.


FACTS

- a. The first set of Board policies was approved by the Board on July 16, 2015. A second set of Board policies was approved by the Board on October 15, 2015.
- b. Each policy was evaluated and assigned to the appropriate Board Committee for oversight of the monitoring process.
- c. The Governance Committee is responsible for evaluating Board Policy SD-12: Information Management and Security.
- d. The Governance Committee has reviewed and accepted the SD-12: Information Management and Security Monitoring Report and finds that OPPD is taking reasonable and appropriate measures to comply with the policy.


ACTION

The Governance Committee recommends Board approval of the 2022 SD-12: Information Management and Security Monitoring Report.

RECOMMENDED:

DocuSigned by:

51E67D98FF081470...
Kathleen W. Brown
Vice President and Chief Information Officer

APPROVED FOR BOARD CONSIDERATION:

DocuSigned by:

AC399FDCE56247E...
L. Javier Fernandez
President and Chief Executive Officer

Attachments:
Exhibit A – Monitoring Report
Resolution



SD-12: Information Management and Security Monitoring Report

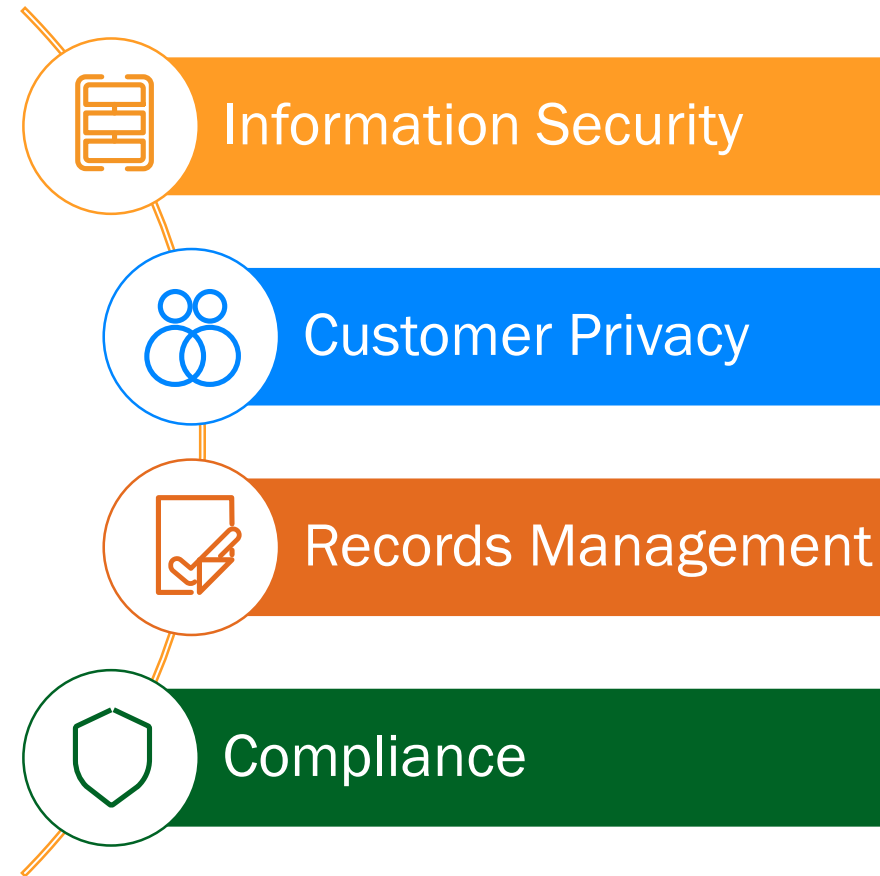
Kate Brown

Vice President and Chief Information Officer

October 18, 2022

SD-12: Information Management & Security

- Robust information management and security practices are critical to effective risk management and to ensure regulatory compliance, business resiliency and customer-owner satisfaction
- OPPD shall safeguard and protect data, information and assets from inappropriate use, improper disclosure and unauthorized release



Ensuring Compliance to SD-12



Information Security



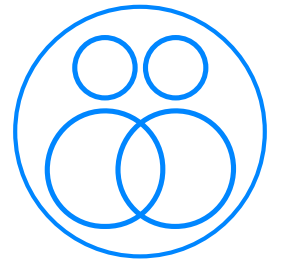
Objective

- OPPD will implement processes and methodologies to protect print, electronic, or any other form of information or data from unauthorized access, misuse, disclosure, destruction, or modification

Ongoing Controls

- Maturing our capabilities to identify and respond to cybersecurity events
- Identifying and mitigating known vulnerabilities based on risk to the organization
- Conducting regular cybersecurity incident response exercises to test and improve our processes
- Establishing and maturing plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events
- Leveraging partnerships to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience
- Maturing our security awareness services with a focus on phishing prevention
- Creating security awareness to all employees through training and communications

Customer Privacy



Objective

- Except as provided by law or for a business purpose, OPPD will not disseminate customer-owner information to a third party for non-OPPD business purposes without customer-owner consent
- Where sensitive and confidential information is disseminated for a business purpose, OPPD will ensure that the third party has information practices to protect the sensitive and confidential customer-owner information
- OPPD will maintain a process that identifies the business purposes for which OPPD will collect, use and disseminate sensitive and confidential customer-owner information

Ongoing Controls

- OPPD's Identity Theft Prevention Program is the cornerstone for ensuring customer privacy throughout OPPD
 - This program is reviewed regularly for effectiveness and compliance with state and federal regulations
 - An annual report of this program is reviewed by OPPD management to ensure its effectiveness
 - All employees with access to customer information are trained based on this program, including annual training and regular assessments in relation to data sharing and security
- Customer Service and Public Affairs partner to provide customer communications based on fraud-related trends and events

Records Management



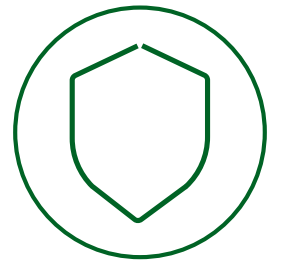
Objective

- The efficient and systematic control of the creation, capture, identification, receipt, maintenance, use, disposition, and destruction of OPPD records, in accordance with legal requirements

Ongoing Controls

- Strengthening records management collaboration across OPPD to become an enterprise function
- Ensuring records management staff are trained on practices and have procedures for maintaining, archiving and destruction of required business records
- Leveraging industry and external partnerships, including outside utilities and government entities
- Continuing process and service improvements in light of efficiency, effectiveness and security
- Supporting records management efforts associated with FCS nuclear decommissioning and other EPND activities

Compliance – Ongoing Controls



Objective

- Comply with contractual and legal requirements through the use of technical controls, system audits and legal review

Ongoing Controls

- Strengthening governance, risk and compliance capabilities through formal enterprise management, identification and attestations of control compliance
- Engaging employees, legal counsel and external entities to stay abreast of the changing landscape from a legal/compliance perspective
- Confirming that security and privacy measures are included in contracting processes for the protection of OPPD data and systems, and also supported by our engaged third parties
- Performing internal and external audits and reviews on a regular basis, with findings provided to management

Progress in 2022

Information Security

- Continued specialized training and awareness activities
- Advanced threat detection and prevention
- Strengthened security and technical controls in alignment with technology usage
- Enhanced incident response and disaster recovery
- Sustained strong local, state, federal industry and data sharing partnerships
- Strengthening governance and management of enterprise information security capability maturity

Records Management

- Continued development of records management function
- Completed retention schedule review, received State of Nebraska Records Management Office approval
- Established Data Management Policy
- Continued support of records management efforts associated with FCS nuclear decommissioning and EPND activities

Information Management & Customer Privacy

- Expanded partnership and collaboration across the organization to further strengthen privacy by design, data management and governance
- Sustained partnerships to help detect and prevent suspicious activity
- Reviewed industry trends in alignment with strategic initiatives
- Partnership with expert industry leaders in data management and governance.

Compliance

- Further strengthened security policy (and associated controls), further aligning to established best practices, industry standards, and regulatory recommendations and requirements
- Continued focus on digital transformation, cloud technology growth and OT/IT convergence
- Annual internal and external maturity assessments of critical capabilities, threat and vulnerability management
- Increased focus on measurement, metrics and testing

Recommendation

- The Governance Committee has reviewed and accepted this Monitoring Report for SD-12 and recommends that the Board finds OPPD is taking reasonable and appropriate measures to comply with Board Policy SD-12.

**Any additional reflections on
what has been
accomplished ... or
challenges or gaps**

