

Bogner/Brown

RESOLUTION NO. 6670

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: Security and Information Management on an annual basis. The Committee has reviewed the 2024 SD-12: Security and Information Management Monitoring Report and finds OPPD to be sufficiently in compliance with the policy as stated.

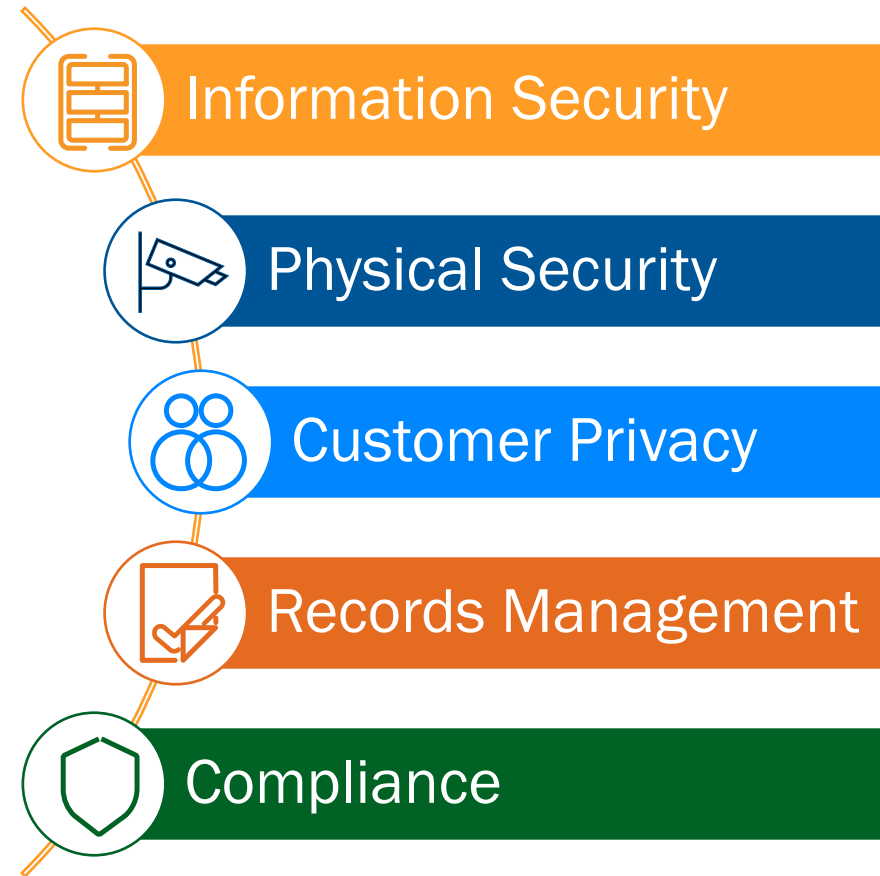
NOW, THEREFORE, BE IT RESOLVED that the Board of Directors of Omaha Public Power District hereby accepts the 2024 SD-12: Security and Information Management Monitoring Report, in the form as set forth on Exhibit A attached hereto and made a part hereof, and finds OPPD to be sufficiently in compliance with the policy as stated.

SD-12: Security and Information Management Governance Committee Report November 19, 2024

Kathleen Brown
CIO and VP Technology and Security

SD-12: Security and Information Management

Robust security and information management practices are critical to effective risk management and to ensure regulatory compliance, business resiliency and customer-owner satisfaction, and the safeguarding of people and facilities.



Ensuring Compliance to SD-12



Information Security



Objective

- Processes and methodologies protect print, electronic, or any other form of information or data from unauthorized access, misuse, disclosure, destruction or modification.

Ongoing Controls

- Advancing our capabilities to identify and respond to cybersecurity events
- Identifying and mitigating new and aging known vulnerabilities based on risk to the organization
- Conducting regular cybersecurity incident response exercises to test and improve our processes and updating the incident response plan
- Leveraging partnerships to collect and analyze cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience
- Maturing our security awareness services with a focus on enhanced training and email phishing prevention
- Increasing security awareness to all employees through ongoing communications
- Leading and participating in security organizational roles and exercises

Physical Security

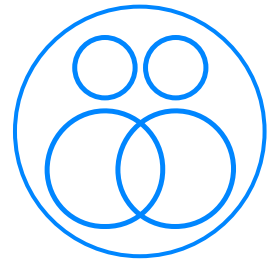


Objective

- A safe and secure environment for all OPPD personnel, contractors, visitors, operations and properties.
- Security processes support emergency management, vulnerability and behavioral threat management programs, and utilize applicable national, industrial and communications security best practices.

Ongoing Controls

- Implementing Critical Infrastructure Protection 014 (CIP-014) compliance and Enterprise Security Improvement Program (ESIP) projects, including auditing of processes and standards
- Collaborating with Nebraska Information & Analysis Center and law enforcement agencies
- Documenting remediation and compensatory measures for deviations of security practices allowing for operational flexibility
- Performing threat and vulnerability assessments of assets
- Conducting security awareness education and training campaign for employees, contractors and visitors
- Collaborating with Utility Operations, Customer Service and Emergency Management



Customer Privacy

Objective

- Customer privacy and protection of customer-owner information, preventing any dissemination of customer-owner information to a third party for non-OPPD business purposes without customer-owner consent or except as provided by law or for a business purpose.

Ongoing Controls

- Ensuring customer privacy through OPPD's Identity Theft Prevention Program
 - Reviewing this program annually for effectiveness and compliance with state and federal regulations
 - Reviewing an annual report of this program by OPPD management to ensure its effectiveness
 - Training all employees with access to customer information on this program, including annual training and regular assessments in relation to data sharing and security
- Providing customer communications regarding fraud-related trends and events in partnership with Customer Service and Public Affairs

Records Management



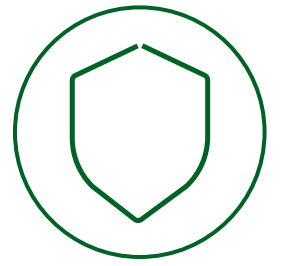
Objective

- Efficient and systematic control of OPPD records inclusive of, identification, classification, storage, security, retrieval, tracking and destruction or permanent preservation of records.

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
- Improving processes and services in consideration of efficiency, effectiveness and security
- Supporting records management efforts associated with Fort Calhoun Station nuclear decommissioning and other Utility Operations activities

Compliance



Objective

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

Ongoing Controls

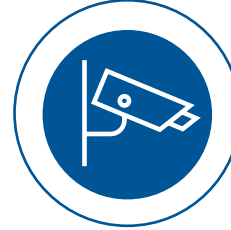
- Strengthening governance, risk and compliance capabilities through formal enterprise management, identification and attestations of control compliance
- Engaging employees, legal counsel and external entities to stay abreast of the changing landscape from a legal/compliance perspective
- Confirming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

2024 Accomplishments



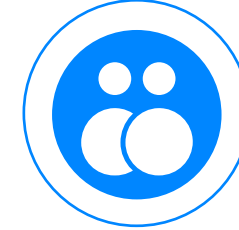
Information Security

- ✓ Rewrote and published OPPD Cybersecurity Incident Response Plan
- ✓ Deployed new email and file system security technological tools
- ✓ Processed and reviewed security incidents & threat intelligence reports



Physical Security

- ✓ Completed majority of CIP 014 required assets
- ✓ Continued security enhancement and upgrades
- ✓ Resolved audit remediations
- ✓ Performed physical security vulnerability assessments
- ✓ Expanded security camera views



Customer Privacy

- ✓ Completed Data Governance Charter and formed Steering Committee
- ✓ Created Data Governance roadmap, policy, framework and operating model
- ✓ Implemented access controls to data

2024 Accomplishments



Records Management

- ✓ Implemented process improvement to clear multi-year record archival backlog
- ✓ Transmitted 364 records of more than 190,000 pages required for nuclear compliance
- ✓ Digitized Master Facility Plan



Compliance

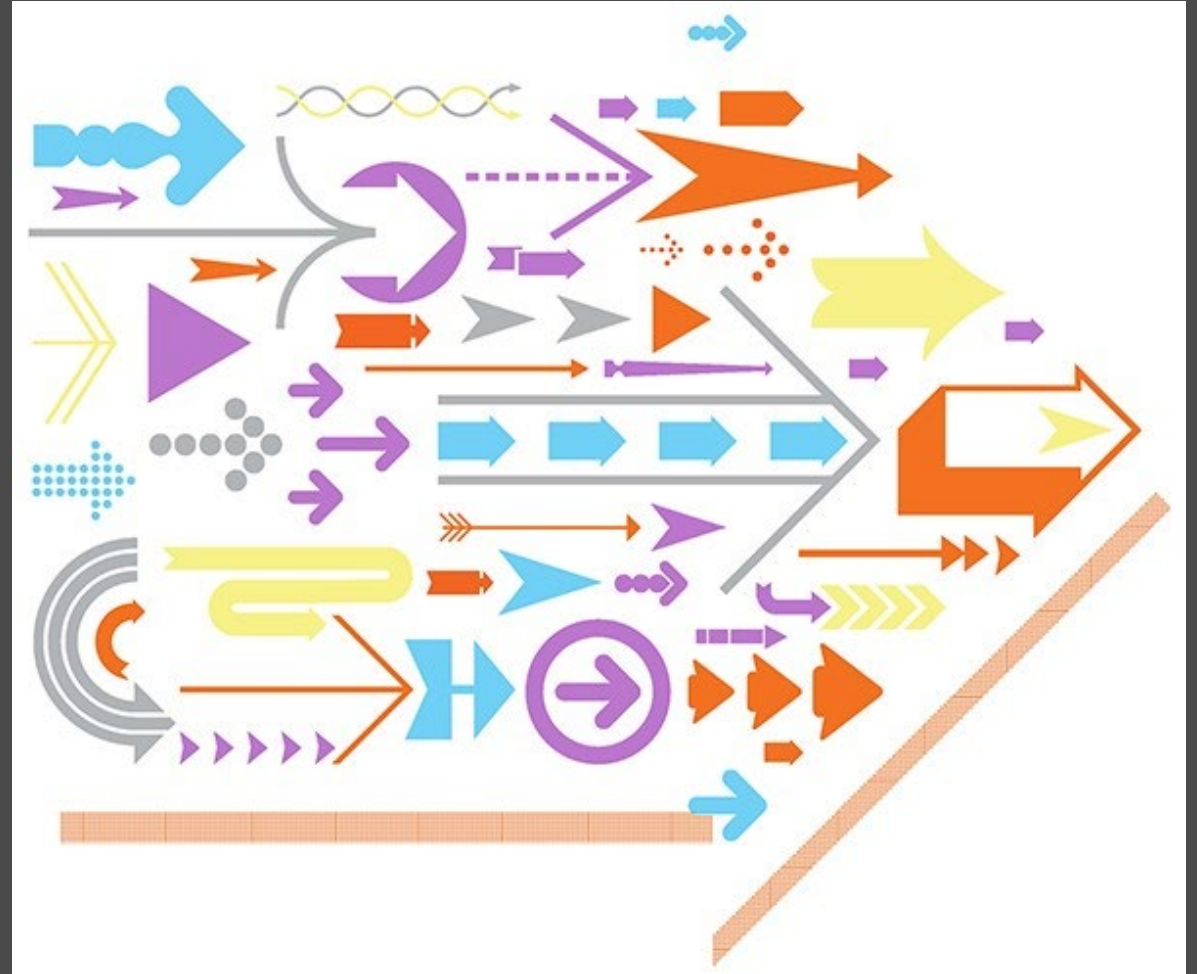
- ✓ Participated in an industry peer review
- ✓ Validated federal compliance with HIPAA
- ✓ Researched requirements for compliance with two new Nebraska laws

Recommendation

The Governance Committee has reviewed and accepted this Monitoring Report for SD-12: Security and Information Management and recommends that the Board finds OPPD to be sufficiently in compliance with Board Policy SD-12: Security and Information Management.

Any reflections on

**what has been
accomplished, challenges
and/or strategic
implications?**





Action Item

BOARD OF DIRECTORS

November 19, 2024

ITEM

SD-12: Security and Information Management Monitoring Report

PURPOSE

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

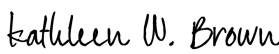
FACTS

- 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: Security and Information Management.
- d. The Governance Committee has reviewed and accepted the SD-12: Security and Information Management 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 2024 SD-12: Security and Information Management Monitoring Report.

RECOMMENDED:

DocuSigned by:

6413656A44F34CF
 Kathleen W. Brown
 Vice President and Chief Information Officer

APPROVED FOR BOARD CONSIDERATION:

Signed by:

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

Attachments:
 Exhibit A – Monitoring Report
 Resolution