Omaha Public Power District

SD-12: Information Management and Security Monitoring Report

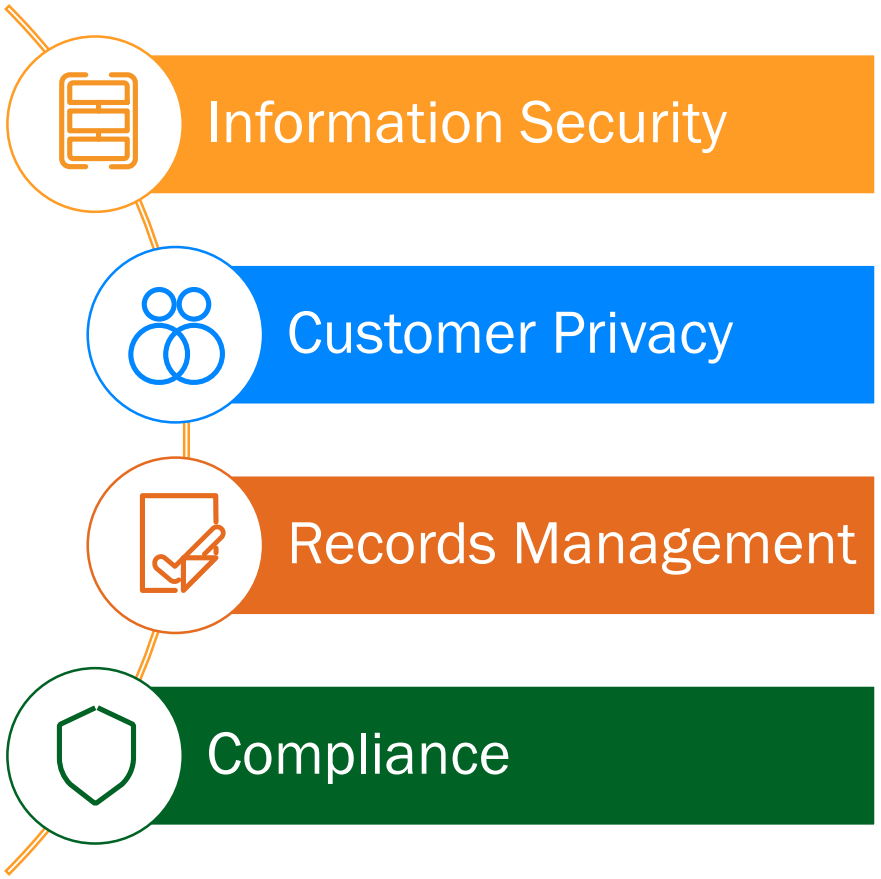
Governance Committee Report

October 13, 2020

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

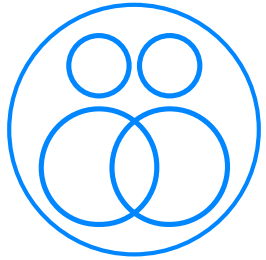
Objective

- 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 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 teams partner to provide customer communications based on fraud-related trends and events

Records Management

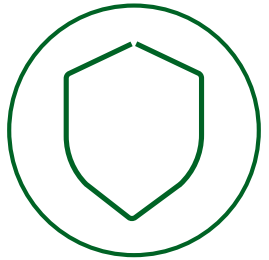
Objective

- 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

- 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 such as Nebraska Public Power District and State of Nebraska
- Continuing process and service improvement in light of efficiency, effectiveness and security
- Strengthening collaboration across OPPD in the area of records management
- Supporting records management efforts associated with FCS nuclear decommissioning activities

Compliance – Ongoing Controls



Objective

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

Ongoing Controls

- Developing program for policy governance, procedures and standards
- 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 included in contracting processes for the protection of OPPD data and systems provided by or supported by third parties
- Performing internal and external audits and reviews on a regular basis and reports on findings provided to management

Progress in 2020

Information Security

- Assessed impact of successful ransomware attacks
- Joined Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP)
- Evaluated security threat from changes from COVID-19
- Made progress on 2020 initiatives
- Participated in cybersecurity incident response exercises

Records Management

- Continue redesign of records management function
- Completed retention schedule review, seeking State of Nebraska Records Management Office approval
- Leverage industry and external partnerships
- Support records management effort associated with FCS nuclear decommissioning activities

Customer Privacy

- Partnered to proactively shut down toll free numbers known to be used in attempt to defraud OPPD customers
- Formed local utility partnership with LES & NPPD to alert each other of area scam activities
- Joined Utilities United Against Scams (UUAS)
- Developing self-service reporting

Compliance

- Created new BTBS policy framework
- Developed security and privacy controls in our supply chain processes, including our vendor selection and contract processes
- Leveraged enterprise change management and corporate communications for socialization of changes

Recommendation

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

Questions