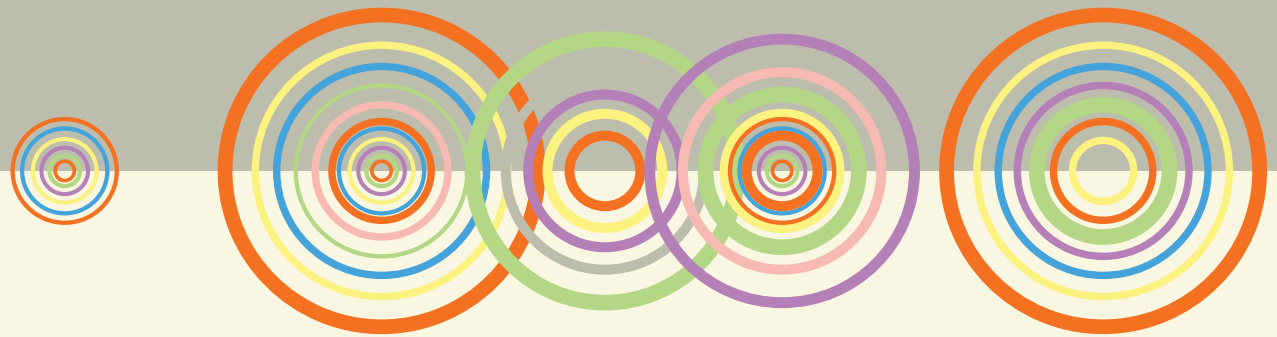
Exhibit A

SD-12: SECURITY AND INFORMATION MANAGEMENT MONITORING REPORT RISK COMMITTEE

12.16.25



Kate Brown
CIO & VP, Technology & Security

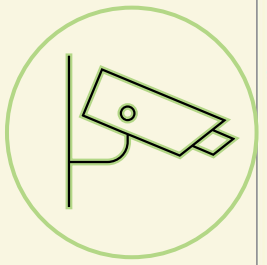
OPPD
Omaha Public Power District

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

PHYSICAL SECURITY



Objective

- OPPD will provide 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 Federal Bureau of Investigation (FBI), U.S. Department of Homeland Security (DHS), 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 personnel, assets and operations
- De-escalation training for applicable employees and contractors

INFORMATION SECURITY

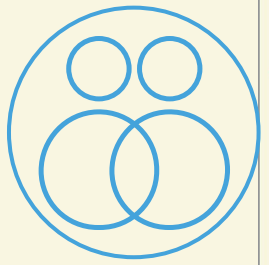
Objective

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

Ongoing Controls

- Establishing data governance and data classification roles to ensure data and information accountability
- Identifying and mitigating new and aging known vulnerabilities based on risk to the organization
- Conduct cybersecurity incident response exercises to test and improve our processes and updating the incident response plan
- Leveraging local, state and national partnerships to collect and analyze cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience
- Increasing security awareness through ongoing communications, enhanced training, email phishing prevention, and implementing Information Classification policies and standards

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

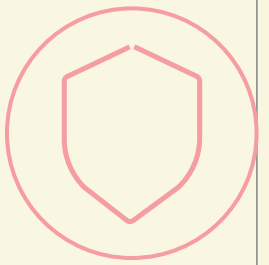
Objective

- Efficient and systematic control of OPPD records through the implementation of a comprehensive document and records management framework.

Ongoing Controls

- Leveraging strategic partnerships across the industry, including collaborations with peer utilities and governmental entities.
- Drive continuous improvement in records and document management practices
- Foster cross-functional collaboration to sustain alignment with enterprise-wide process optimization goals.
- Supporting the management and governance of nuclear records in alignment with Fort Calhoun Station decommissioning activities.

COMPLIANCE



Objective

- Technology compliance with contractual and legal requirements using technical controls, system audits and legal review.

Ongoing Controls

- Enhancing security governance, risk and compliance maturity through the formalization of risk management practices, identification of control gaps, with sustained compliance and accountability
- 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 contracts for the protection of OPPD data and systems, and are supported by our third parties
- Performing annual external audits and internal reviews, and providing findings and identified mitigation actions to management

2025 ACCOMPLISHMENTS

PHYSICAL SECURITY

- ✓ Completed physical security upgrades at a CIP-014 location
- ✓ Performed physical security vulnerability assessments
- ✓ Expanded security controls and presence at new generation assets
- ✓ Enhanced security controls at the Huddle Space
- ✓ Provided security awareness updates to Executive Leadership Team and Board members
- ✓ Provided Active Threat and De-escalation training

INFORMATION SECURITY

- ✓ Strengthened multi-factor authentication (MFA)
- ✓ Enhanced security logging and monitoring capability
- ✓ Improved process for immediate cyber vulnerabilities
- ✓ Integrated select applications in OPPD's identity security tool
- ✓ Established a data governance program, steering committee and applicable policies

CUSTOMER PRIVACY

- ✓ Implemented access controls to customer applications and associated data
- ✓ Enhanced myAccount customer protections
- ✓ Completed customer data protection training

2025 ACCOMPLISHMENTS

RECORDS MANAGEMENT

- ✓ Transformed the Oracle WebCenter content management system into a legally defendable, compliant, and scalable solution for long-term digital archival storage.
- ✓ Digitized OPPD's physical hard copy storage vault to ensure long-term preservation, streamlined access, and compliance with archival standards.

COMPLIANCE

- ✓ Completed an on-site NERC Critical Infrastructure Protection Audit, covering both cyber and physical security standards.
- ✓ Implementation of document and records management programs which meet or exceed recommended Records and Information Management (RIM) industry standards.

RECOMMENDATION

The Risk 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.

Any reflections on

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