

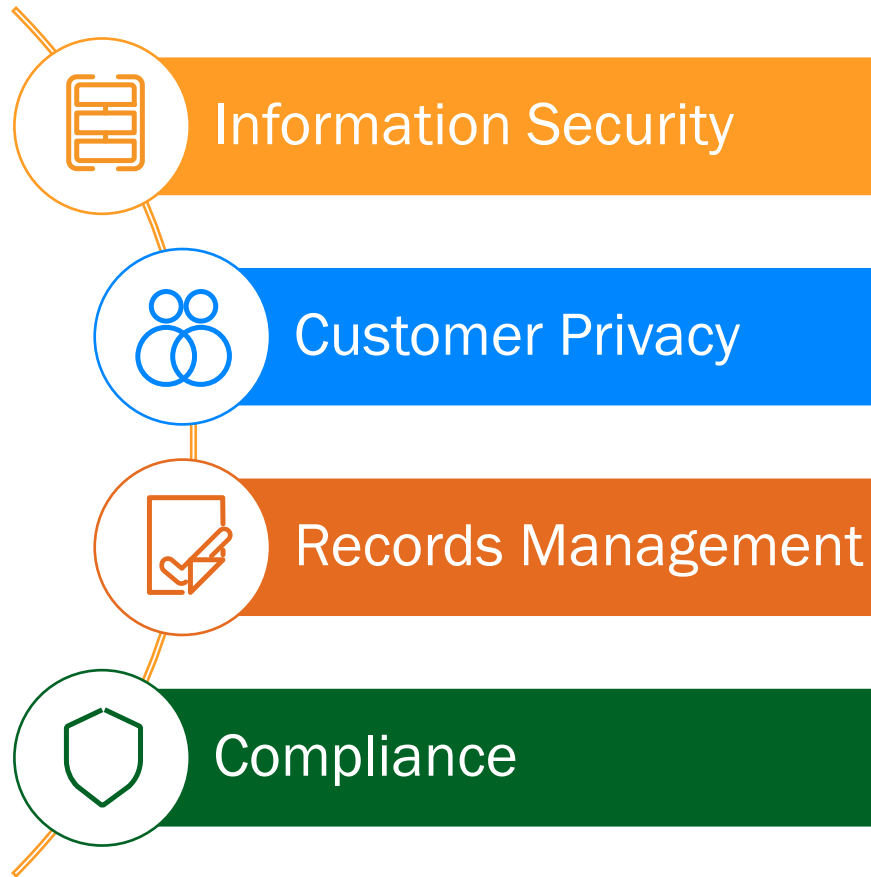


SD-12: Information Management and Security Governance Committee Report November 2023

Kate Brown
CIO & Vice President, Technology & Security

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



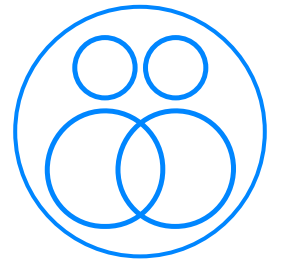
Objective

- 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

- Leverage procedures and technologies, and advance our capabilities to detect, analyze and respond to cybersecurity events
- Identify and mitigate known vulnerabilities based on risk to the organization
- Conduct regular cybersecurity incident response exercises to test and improve our processes
- Work with partners to share cybersecurity information, increase awareness of threats and vulnerabilities, and help to reduce risks and increase operational resilience
- Strengthen security awareness services with a focus on phishing prevention
- Increase 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 that protect 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.
 - Employees with access to customer information are trained annually on this program and are regularly assessed 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



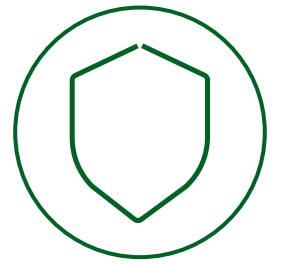
Objective

- 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

- Strengthen records management collaboration across OPPD to become an enterprise function
- Ensure records management staff are trained on practices and have procedures for properly maintaining, archiving and destroying business records per defined retention practices
- Leverage industry and external partnerships, including other utilities and government entities
- Improve processes and services in consideration of efficiency, effectiveness and security
- Support records management work related to FCS nuclear decommissioning & other Utility Operations activities

Compliance – Ongoing Controls



Objective

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

Ongoing Controls

- Strengthen governance, risk and compliance capabilities through formal enterprise management, identification and attestations of control compliance
- Engage employees, legal counsel and external entities to stay abreast of the changing landscape from a legal/compliance perspective
- Confirm 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
- Perform internal and external audits and reviews on a regular basis, with findings provided to management

Progress in 2023

Information Security



- Emphasized realistic and timely training, awareness and phishing activities
- Continued use of threat detection and prevention tools
- Strengthened management of enterprise information security maturity via gap analysis
- Increased data center capabilities
- Improved alignment of incident response and disaster recovery processes

Records Management



- Moved records management function to Legal Operations department
- Upgraded records management software to enable greater security, legal compliance, overall records processing and centralized content management
- Improved access control to records repository
- Continued records management efforts associated with FCS nuclear decommissioning and Utility Operations activities

Information Management & Customer Privacy



- Successfully hired for new position: Data Governance Program Manager
- Created Data Governance Charter
- Establishing a Data Governance Council
- Continued development of lifecycle management practices
- Deploying an Identity & Access Management (IAM) platform to strengthen access control

Compliance



- Implemented additional security policies and standards
- Participated in ongoing internal audit activities
- Legal Operations revised Legal Hold and records management processes for security and compliance purposes
- Continued development and system upgrades related to digital transformation, cloud technology growth and OT/IT convergence

Recommendation

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

