Your Energy Partner®
OPPD
Omaha Public Power District

Exhibit C

SD 12: Information Management and Security Board Policy Refinement Discussion February 13, 2024

Kate Brown
CIO and Vice President Technology & Security

SD 12: Information Management and Security

Your Energy Partner® OPPD Omaha Public Power District	**OMAHA PUBLIC POWER DISTRICT** **Board Policy**	**Category:**	Strategic Direction
	Policy No. and Name: SD-12: Information Management and Security	**Monitoring Method:**	Governance Committee Board Report
		Frequency:	Annually
Date of Approval:	October 15, 2015 March 10, 2016 October 13, 2016	**Resolution No.:**	6082 6114 6146

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.

OPPD shall take prudent and reasonable measures to ensure:

- *Information Security:* 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.
- *Customer Privacy:* 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.
- *Records Management:* The efficient and systematic control of OPPD records inclusive of, identification, classification, storage, security, retrieval, tracking and destruction or permanent preservation of records.
- *Compliance:* Comply with contractual and legal requirements through the use of technical controls, system audits and legal review.

"Governance exists in order to translate the wishes of an organization's owners into organizational performance."
- John Carver

Refinement Process: Strategic Directives

BOARD WORK PLAN

Step 1
Committee chair/director requests during regular All Committee to determine if policy refinement will be added to the Board Work Plan.

PRIORITIZATION

Step 2
Board Chair and CEO convene to confirm priority, resource requirements, and start and finish dates; pending discussion, Chair/CEO will inform committee chair.

PRES & CEO

Step 3
Assigns ELT to policy refinement as appropriate; approves initial drafts for committee review and comment.

COMMITTEE

Steps 4-5
Reviews, revises and finalizes refinements to present to Board.

Committee Chair
Committee

BOARD

Steps 6-8
Provides feedback on draft; concur readiness for public posting, if applicable; approve final committee recommendation via Board vote.

In-Committee

Added to Work Plan
11/14/23

Committee discussion & recommendation development
1/11/24

Board review/decision
1/16/24
Public Comment
TBD
Vote
TBD

Today's Discussion

Is there anything that requires further clarification?
Is there anything you especially like?
Is there anything that you'd like the Committee to consider before moving this forward for public review and comment?

Your Energy Partner® OPPD Omaha Public Power District	OMAHA PUBLIC POWER DISTRICT Board Policy	Category:	Strategic Direction
	Policy No. and Name: SD-12: Security and Information Management ~~and Security~~	Monitoring Method:	Governance Committee Board Report
		Frequency:	Annually
Date of Approval:	October 15, 2015 March 10, 2016 October 13, 2016 DRAFT REVISION	Resolution No.:	6082 6114 6146 TBD

Robust security and information management ~~and security~~ 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.

~~OPPD shall safeguard and protect data, information and assets from inappropriate use, improper disclosure and unauthorized release.~~

Therefore, OPPD shall take prudent and reasonable measures to ensure:

- 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.
- ~~*Information Security:* OPPD will implement p~~Processes and methodologies ~~to~~ protect print, electronic, or any other form of information or data from unauthorized access, misuse, disclosure, destruction, or modification.
- Customer p~~P~~rivacy~~: Except as provided by law or for a business purpose, OPPD and will~~ not disseminate 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.
- ~~*Records Management:* The e~~Efficient and systematic control of OPPD records inclusive of, identification, classification, storage, security, retrieval, tracking and destruction or permanent preservation of records.
- ~~*Compliance:* Comply~~ Technology compliance with contractual and legal requirements through the use of technical controls, system audits and legal review.

Your Energy Partner® OPPD Omaha Public Power District	OMAHA PUBLIC POWER DISTRICT Board Policy	Category:	Strategic Direction
	Policy No. and Name: SD-12: Security and Information Management	Monitoring Method:	Governance Committee Board Report
		Frequency:	Annually
Date of Approval:	October 15, 2015 March 10, 2016 October 13, 2016 DRAFT REVISION	Resolution No.:	6082 6114 6146 TBD

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.

Therefore, OPPD shall take prudent and reasonable measures to ensure:

- 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.
- Processes and methodologies protect print, electronic, or any other form of information or data from unauthorized access, misuse, disclosure, destruction, or modification.
- Customer privacy and not disseminate 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.
- Efficient and systematic control of OPPD records inclusive of, identification, classification, storage, security, retrieval, tracking and destruction or permanent preservation of records.
- Technology compliance with contractual and legal requirements through the use of technical controls, system audits and legal review.

Next Steps

- Determine if committee is ready to review with the Board and if a public review/comment period is desired. (Governance Committee)
- Confirm target date for Board vote. (Governance Committee)