centralpoint

Data Protection Policy

Protection against inappropriate data leaks, also known as data leakage prevention (DLP), is a critical aspect of Oxcyon's internal processes in place for both Oxcyon and technology partners in part of the overall Information Security plan and policies. Data leaks can occur through various means, including accidental sharing of sensitive information, malicious actions by insiders or external attackers, or vulnerabilities in software and systems. To prevent inappropriate data leaks, Oxcyon has implemented a range of measures and best practices:

1. Data Classification: Classifying data based on its sensitivity. This helps in identifying what needs the highest level of protection. For example, personal, financial, or health data might be classified as highly sensitive, while public information may not require as much protection.

2. Data Inventory: Maintain an inventory of all the data your organization collects, processes, and stores. Knowing where your data resides is crucial for implementing effective protection measures.

3. Access Control: Implement strict access controls to ensure that only authorized personnel can access sensitive data. Use role-based access control (RBAC) and least privilege principles to limit access to the minimum necessary for employees to perform their duties.

4. Encryption: TDE Encryption is used when transferring data in and out of Centralpoint (MS SQL) 2019 Encrypt sensitive data both in transit and at rest. Use strong encryption algorithms and key management practices to protect data from unauthorized access, even if it falls into the wrong hands. https://www.oxcyon.com/Uploads/Public/Documents/SQL%202019%20TDE%20Encryption%20and%20Database%20Restore%20Procedure.pdf

5. User Education and Awareness: Oxcyon trains employees in data security best practices. Teach them how to recognize and respond to phishing attacks, social engineering attempts, and other tactics that can lead to data leaks.

6. Data Loss Prevention (DLP) Solutions: Implement DLP solutions that can monitor and enforce data security policies. These tools can identify and block unauthorized data transfers or leaks, whether intentional or accidental. (Rackspace handles this for external purposes)

7. Data Masking/Anonymization: When sharing data with third parties or for testing purposes, consider using data masking or anonymization techniques to protect sensitive information while still allowing necessary access.

8. Network Segmentation: Segmentation within network(s) to limit the flow of sensitive data and create barriers that prevent unauthorized access or lateral movement by attackers.

9. Logging and Monitoring: Robust logging and monitoring systems to detect suspicious activities or access to sensitive data. Analyze logs regularly for any signs of data leaks or security breaches.

10. Incident Response Plan: Develop a comprehensive incident response plan that outlines how your organization will react in case of a data leak. This should include steps for containment, investigation, notification, and recovery.
Incident flow chart https://www.oxcyon.com/Uploads/Public/Documents/ServerDocs/incident-flowchart.pdf
Incident Response Policy
https://www.oxcyon.com/Uploads/Public/Documents/ServerDocs/IncidentResponseProcedure.docx

11. Regular Auditing and Assessments: Conduct regular security audits and assessments to identify vulnerabilities and weaknesses in your data protection measures. Address any issues promptly.

12. Compliance with Regulations: Ensure that your data protection practices comply with relevant data protection regulations and standards, such as GDPR, HIPAA, or PCI DSS, depending on your industry and location.
https://www.oxcyon.com/centralpoint-dxp/technical-documents-certificates

13. Data Retention and Disposal: Oxcyon has Implemented policies for the proper retention and secure disposal of data that is no longer needed. This reduces the risk of data leaks from outdated or unnecessary information.

14. Remote Work Security: Oxcyon utilized a variety of remoted tools to supports remote work, ensure that remote access is secured through VPNs, multi-factor authentication (MFA), and secure collaboration tools.
https://www.oxcyon.com/centralpoint-dxp/technical-documents-certificates

15. Vendor Risk Management: Assess the security practices of third-party vendors and partners who have access to your data. Ensure they have robust security measures in place to prevent data leaks.

Protection against inappropriate data leaks is an ongoing process that requires a combination of technology, policies, and employee awareness. It's essential to adapt and evolve your data protection strategy as new threats and technologies emerge.

Questions

All questions about this outline or any other areas regarding Information Technology should be directed to the Chief Information Officer (CIO), who can be contacted at mkerchenski@oxcyon.com

Revision History

Date of Change	Responsible	Summary of Change
June 2023	Oxcyon Policy Team	No changes, semi annual review.