Data leak worksheet

Incident summary: A sales manager shared access to a folder of internal-only documents with their team during a meeting. The folder contained files associated with a new product that has not been publicly announced. It also included customer analytics and promotional materials. After the meeting, the manager did not revoke access to the internal folder, but warned the team to wait for approval before sharing the promotional materials with others.

During a video call with a business partner, a member of the sales team forgot the warning from their manager. The sales representative intended to share a link to the promotional materials so that the business partner could circulate the materials to their customers. However, the sales representative accidentally shared a link to the internal folder instead. Later, the business partner posted the link on their company's social media page assuming that it was the promotional materials.

Control	**Least privilege**
Issue(s)	*The data leak incident resulted from a breakdown in implementing the principle of least privilege. The sales manager granted access to a folder of internal documents that included sensitive new product information to the team. This unrestricted access led to the accidental sharing of confidential data with a customer, which later made its way to social media.*
Review	*NIST SP 800-53: AC-6 emphasizes the importance of enforcing least privilege, limiting user access to only what is necessary for their roles, and regularly auditing user privileges to prevent unauthorized access to sensitive information.*
Recommendation(s)	*Automated Revocation: Implement an automated access revocation system that enforces time-limited access to sensitive folders. This ensures*

	that access is automatically revoked when it's no longer needed, reducing the risk of prolonged access to confidential information. *Access Logging and Monitoring: Enhance access controls by introducing comprehensive access logs and monitoring systems. This allows for real-time visibility into who accessed what, aiding in detecting and preventing unauthorized sharing of internal documents.*
Justification	*The recommended control enhancements directly address the issues that led to the data leak. Automated revocation ensures that access to sensitive folders is automatically removed when no longer necessary, preventing users from inadvertently sharing confidential information. Access logging and monitoring provide real-time oversight, allowing for the swift detection and prevention of unauthorized access, minimizing the risk of data leaks. These enhancements align with the principles outlined in NIST SP 800-53: AC-6, ensuring a robust least privilege policy and enhancing information privacy controls.*

Security plan snapshot

The NIST Cybersecurity Framework (CSF) uses a hierarchical, tree-like structure to organize information. From left to right, it describes a broad security function, then becomes more specific as it branches out to a category, subcategory, and individual security controls.

Function	Category	Subcategory	Reference(s)
Protect	PR.DS: *Data security*	PR.DS-5: *Protections against data leaks.*	NIST SP 800-53: AC-6

In this example, the implemented controls that are used by the manufacturer to protect against data leaks are defined in NIST SP 800-53—a set of guidelines for securing the privacy of information systems.

Note: References are commonly hyperlinked to the guidelines or regulations they relate to. This makes it easy to learn more about how a particular control should be implemented. It's common to find multiple links to different sources in the references columns.

NIST SP 800-53: AC-6

NIST developed SP 800-53 to provide businesses with a customizable information privacy plan. It's a comprehensive resource that describes a wide range of control categories. Each control provides a few key pieces of information:

- **Control:** A definition of the security control.
- **Discussion:** A description of how the control should be implemented.
- **Control enhancements:** A list of suggestions to improve the effectiveness of the control.

AC-6	**Least Privilege**
	Control: Only the minimal access and authorization required to complete a task or function should be provided to users.
	Discussion: Processes, user accounts, and roles should be enforced as necessary to achieve least privilege. The intention is to prevent a user from operating at privilege levels higher than what is necessary to accomplish business objectives.
	Control enhancements: ● Restrict access to sensitive resources based on user role. ● Automatically revoke access to information after a period of time. ● Keep activity logs of provisioned user accounts. ● Regularly audit user privileges.

Note: In the category of access controls, SP 800-53 lists least privilege sixth, i.e. AC-6.