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)	*What factors contributed to the information leak?* ***Access Retention:*** *The sales manager did not revoke access to the internal folder after the meeting, leading to continued access by team members who no longer needed it.* ***Communication Breakdown:*** *The sales manager's instruction to wait for approval before sharing promotional materials was unclear, leading to confusion among team members about when and what they could share.* ***Link Mismanagement:*** *The sales representative mistakenly shared a link to the entire internal folder instead of just the promotional materials.* ***Lack of Access Controls for External Sharing:*** *No safeguards prevented external access when a confidential link was shared outside the organization.*

Review	*What does NIST SP 800-53: AC-6 address?* ***NIST SP 800-53: AC-6*** *addresses* ***least privilege*** *as a foundational control, requiring that information system access rights be restricted to only the permissions necessary for users to perform their responsibilities. This includes implementing controls to prevent unauthorized access to sensitive information and to restrict access rights after they are no longer neede*
Recommendation(s)	*How might the principle of least privilege be improved at the company?* ***Improvements to the Principle of Least Privilege:*** ○ *Implement* ***role-based access controls (RBAC)*** *to limit document access based on specific job responsibilities and dynamically adjust permissions based on user needs.* ○ *Enforce* ***automatic expiration of access*** *to sensitive folders after specific time intervals or when access is no longer required.* ○ *Establish* ***multi-level authorization*** *for sharing sensitive information externally, including a review of links shared outside the organization.* ○ *Integrate* ***data loss prevention (DLP) tools*** *that monitor and restrict information-sharing with external parties.* ***Justification*** *These improvements would directly address the identified issues by reducing the likelihood of accidental or unauthorized access to sensitive information. Automatic access expiration and multi-level authorization ensure that access rights are actively managed, limiting the potential for*

	mistakes. DLP (data loss protection) tools further provide checks on information-sharing practices, ensuring that only authorized content is accessible externally. Together, these measures reinforce a robust least privilege approach, protecting against future leaks.
Justification	*How might these improvements address the issues?* *These improvements would directly address the identified issues by reducing the likelihood of accidental or unauthorized access to sensitive information. Automatic access expiration and multi-level authorization ensure that access rights are actively managed, limiting the potential for mistakes. DLP tools further provide checks on information-sharing practices, ensuring that only authorized content is accessible externally. Together, these measures reinforce a robust least privilege approach, protecting against future leaks.*

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

The **NIST Cybersecurity Framework (CSF)** outlines this structure for organizing security functions, with controls like **AC-6** ensuring the restriction of access based on the principle of least privilege.

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.