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?* The information leak occurred due to multiple oversights and failures in protocol. The manager of the sales department neglected to revoke access to the internal-only folder of documents as required. Additionally, the sales representative failed to verify that the link being shared was free of sensitive data. Furthermore, access to the internal folder was not restricted solely to the sales team and the manager, allowing unintended parties to view sensitive information. Lastly, the business partner mistakenly assumed that the link provided had been sanitized and shared it on social media without proper authorization.
Review	*What does NIST SP 800-53: AC-6 address?* *NIST SP 800-53: AC-6 outlines how organizations can implement the*

	principle of least privilege to protect data privacy. It ensures that users or systems are granted only the minimum access necessary to perform their roles. Additionally, it provides control enhancements designed to strengthen the effectiveness of least privilege, helping organizations reduce the risk of unauthorized access and potential data breaches.
Recommendation(s)	*How might the principle of least privilege be improved at the company?* *The principle of least privilege at the company can be improved by restricting access to sensitive resources based on user roles. For instance, only the manager should have access to the entire folder, while the rest of the team should be limited to the promotional materials needed for their tasks. Additionally, the company could implement a centralized system that allows users to securely access necessary information on designated computers, such as those in a meeting room. User access should be tailored to their security clearance, ensuring that sensitive data is only available to authorized individuals. Regularly auditing user privileges would further strengthen the enforcement of least privilege and minimize risks of unauthorized access.*
Justification	*How might these improvements address the issues?* *These improvements address the issues by reducing the risk of unauthorized access to sensitive information. Restricting access to files based on user roles and security clearance ensures that only employees with the appropriate permissions can access specific data. Implementing a centralized system would further enforce this principle, as access would be granted on a strict need-to-know basis. Additionally, requiring managers and security teams to regularly audit access to team files would help identify and address any inappropriate permissions, preventing data leaks and minimizing the exposure of sensitive information.*

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.