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 occurred due to excessive access permissions and lack of oversight. The manager failed to revoke folder access, and the representative mistakenly shared the entire folder instead of a single file. This resulted in unauthorized external exposure of internal documents.*
Review	*NIST SP 800-53: AC-6 focuses on enforcing the principle of least privilege by ensuring users are only granted access necessary for their roles. It helps prevent data leaks by limiting unnecessary permissions and reducing the risk of accidental or intentional data exposure.*
Recommendation(s)	*Two control enhancements from* ***NIST SP 800-53: AC-6*** *that might have prevented the data leak are:* 1. ***AC-6(1) – Least Privilege | Authorize Access to Security Functions***

	This enhancement ensures that access to security-relevant information and functions is limited to only authorized personnel. Applying this could have restricted the customer success representative's access to sensitive internal documents not needed for their role. 2. ***AC-6(10) – Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions*** *This enhancement prohibits users without elevated permissions from performing actions like broadly sharing internal folders. Implementing it could have prevented the representative from being able to share the entire folder externally.* *Both enhancements enforce tighter control over user permissions and actions, directly supporting the principle of least privilege.*
Justification	*Implementing control enhancements AC-6(1) and AC-6(10) will ensure only authorized users can access or share sensitive data, reducing unnecessary exposure. These controls reinforce least privilege by preventing non-privileged users from executing high-risk actions, which directly addresses the oversight and accidental sharing that led to the initial data leak.*

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.