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)	*There is a folder which contains internal-only documents - that was shared by a sales manager… It was not publicly announced and was meant to be kept confidential until the date of release. During the sales meeting, an employee accidently shared said file which was then circulated through business partners and customers. Along with the misuse of documents the employee was not informed of least privilege.*
Review	*What does NIST SP 800-53: AC-6 address?* *NIST SP 800-53: AC-6 addresses the achievement of least privilege which in theory sets up a control where only the minimal access and authorization required to complete a task or function should be provided to users.*

Recommendation(s)	*How might the principle of least privilege be improved at the company? The confidential file should be kept with a higher security, disallowing users who do not have access thus preventing any data leaks. In addition, we should be able to perform a rigorous security audit maintaining the concept of least privilege, ensuring that those who have access to certain files are at a need-to-know basis.*
Justification	*With the application of NIST SP 800-53: AC-6 we should be able to prevent incidents such as this scenario in the future. This will provide a security net stopping users who should not have confidential information access and allow only those who are authorized to share, view, or edit certain documents/folders.*

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.