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?* *First, the sales manager should not have shared the internal-only documents with their team. They should have made a separate folder, only containing the necessary documents. After the meeting the shared access was not revoked, leaving the information about the new product accessible to everyone. Although they were given a warning, one of the members mistakenly gave access to the said folder with a business partner. And later he posted the link to this internal folder on social media. It was supposed to have contained only promotional materials but it also contained the information that should have been confidential.*
Review	*What does NIST SP 800-53: AC-6 address?* *NIST or National Institute of Standards and Technology is a regulatory*

	agency within the federal government. The act of 2002, specifically the FISMA act or Federal Information Security Management Act directed NIST to develop guidelines to heighten the security measures. These are NIST Special Publication (SP) 800-53. It provides a list of controls that support the development of more secure federal information systems. It comprises over 100 controls. The AC control family consists of information regarding system logging, i.e. who has access to what. *The official control statement for AC-6 is as follows:* ***The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.***
Recommendation(s)	*How might the principle of least privilege be improved at the company?* *The employees should be made more aware of the security practices. They should strictly follow the guideline of which documents and information should be shared with whom and for how long. If they need to share some confidential information, the access should be revoked after a certain period the information is conveyed.*
Justification	*How might these improvements address the issues?* *It is difficult to eradicate all the human errors but if the rules of least privilege are followed it will reduce such risks. The leak that happened was initially caused by sharing of the folder that contained confidential information that should have only been shared separately and not along with the other promotional materials. The access to the confidential material to many people lead to the uneventful incident.*

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.