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?* 1. *Violation of Principle of least privilege,* only the minimal access and authorization required to complete a task or function should be provided to users. 2. *Not being alert and cautious about data security and sharing it across to unauthorized people.* 3. *Not having regular audits of user privileges.*
Review	*What does NIST SP 800-53: AC-6 address?* *NIST SP 800-53: AC-6 addresses "Protections against data leaks", falling under the category of "data security". It further emphasizes on the "Principle of least privilege", stating that* only the minimal access and authorization required to complete a task or function should be provided to

	users. The intention is to prevent a user from operating at privilege levels higher than what is necessary to accomplish business objectives.
Recommendation(s)	*How might the principle of least privilege be improved at the company?* ● 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.
Justification	*How might these improvements address the issues?* 1. *By restricting access to sensitive resources, the "internal-only folder" containing sensitive information, would not have been shared across in the first place. By ensuring this, such mishaps can be minimized in the future.* 2. *By automatically revoking access to the information after a certain period of time, the sales manager could have disabled access to the folder right after the meeting, i.e. after the job was done. This would have prevented further sharing of that resource in the future.* 3. *Having activity logs and conducting regular audits about user privileges helps ensure any accidental data leak in the future, by ensuring that only minimal authorization is given.*

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.