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 main factors that contributed to the information leak were not following the principle of least privilege, and poor separation of duties enforcement. The folder that was shared was only supposed to be viewed by the team working on it, so instead of classifying it as *internal-only*, it should have been classified as *confidential*. Employees should only have access when necessary.

Review	The NIST SP 800-53:AC-6 addresses data security, and protections against data leaks. It controls access and authorization required to complete tasks/functions. Its purpose is to prevent a user from operating at privilege levels higher than what is necessary to accomplish business objectives.
Recommendation(s)	Periodical and consistent monitoring/auditing of user accounts is a key part of maintaining least privilege, and should be implemented immediately. In addition, keeping activity logs of provisioned user accounts and which resources they accessed is crucial. Lastly, access to important information should be automatically revoked after a certain period of time.
Justification	Since the main factors leading up to this incident were failure to implement the principle of least privilege, and separation of duties, our team's recommendations align with the issue. Auditing user accounts ensures all employees are following the guidelines/rules. Keeping activity logs helps security and IT professionals in reviewing any suspicious activity. Finally, automatic revoking of access helps ensure that nobody has access to any material they no longer need to use.

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.