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?* It's determined that the principle of least privilege was not enforced properly by the manager. During the meeting, privilege was enabled by providing employees access to the documents,, but authorization was not revoked upon completion of the initial task.
Review	*What does NIST SP 800-53: AC-6 address?* To reduce risk, the principle of least privilege is addressed to provide access only as needed to perform a specific (operational) task. There are additional security control enhancements in place to further enforce Access Control.

Recommendation(s)	*How might the principle of least privilege be improved at the company?* - Prohibit Privileged Access by Non-organizational Users - Automatically revoke access to information after a period of time
Justification	*How might these improvements address the issues?* It's important to revoke access automatically to avoid a human vulnerability, such as the error made at the end of the internal meeting by the sales manager. The company also needs to enforce prohibited access by non-organizational users so that even if access wasn't automatically removed, there would still be the 2nd control in place.

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.

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.