Data leak worksheet

Incident summary:A sales manager distributed access to a folder containing internal documents, including files related to an unreleased product, customer analytics, and promotional materials, to their team during a meeting. Following the meeting, the manager neglected to revoke access to the internal folder but cautioned the team against sharing the promotional materials without approval.

Subsequently, during a video call with a business partner, a member of the sales team overlooked the manager's warning and intended to provide a link to the promotional materials for circulation to the partner's customers. However, inadvertently, the sales representative shared a link to the internal folder instead. Consequently, the business partner mistakenly posted the link on their company's social media page, assuming it led to the promotional materials.

Control	**Least privilege**
Issue(s)	*Access to the internal folder extended beyond the sales team and the manager, indicating a broader scope of individuals with access. It was inappropriate for the business partner to have been granted permission to disseminate the promotional information on social media.*
Review	*NIST SP 800-53: AC-6 addresses how an organization can protect their data privacy by implementing least privilege. It also suggests control enhancements to improve the effectiveness of least privilege.*
Recommendation(s)	• *Restrict access to sensitive resources based on user role.* • *Regularly audit user privileges.*
Justification	*Preventing data leaks can be achieved by restricting shared links to internal files exclusively for employees. Additionally, implementing regular audits of access to team files by managers and security teams would effectively limit the exposure of sensitive information.*

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.

Note: In the category of access controls, SP 800-53 lists least privilege sixth, i.e. AC-6.