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 factors that contributed to the information leak were the improper authorizations given to the sales team by the sales manager. A lack of appropriate permissions was one factor, another factor was the lack of revoking the team's access to the internal folder.*
Review	*NIST SP 800-53 addresses information privacy. It was developed to provide businesses with a customizable plan to protect information. This set of guidelines includes Access Controls (AC) to apply to your plan. The control NIST SP 800-53: AC-6 is designated to the principle of least privilege. This control enforces that only the minimal access and authorization that is required to complete a task is given to users. The* PR.DS-5 subcategory gives clarity into the *protection of data and aids in the protection against data leaks.*

Recommendation(s)	*To improve the principle of least privilege at this company, I recommend the following:* • *Restrict access to sensitive resources based on user role.* • *Remove access to information after a set time.* • *Employee Training relating to permissions (including managers)* Implement the NIST SP 800-53: AC-6 access control and the PR.DS-5 subcategory. This will address *protection against data leaks and provide a control for the principle of least privilege.*
Justification	*Having access restricted and confidential data limited based on an employees' role/job title/department will ensure they are only allowed to access what they need to perform their job. This will prevent the likelihood of data leaks. Revoking any temporary access to sensitive resources after a period can prevent employees from having access to old projects or folders that they may not need in the future. This can decrease the likelihood of disgruntled employees and untrained employees gaining unnecessary access to files and folders.*

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.