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?* A customer support representative was granted access to a folder containing files associated with a new product offering, including customer analytics and marketing materials. The **manager forgot to rescind access** to this folder following its legitimate use by the representative, meaning the representative was able to share marketing information with a business partner during a sales call. However, **the representative accidentally shared the entire folder**. The business partner received the link to internal documents and **posted it to their social media page** - the private information was now in the public sphere.

Review	*What does NIST SP 800-53: AC-6 address?* AC-6 addresses the principle of least privilege i.e - only the minimal access and authorization required to complete a task or function should be provided to users. Implementation of processes, user accounts and roles with the intention of preventing users from accessing information that is not relevant to their working objectives.
Recommendation(s)	*How might the principle of least privilege be improved at the company?* When reviewing the *NIST SP 800-53: AC-6,* two control enhancements that might have prevented the data leak are: **1)** Automatically revoke access to information after a period of time. **2)** Restrict access to sensitive resources based on user role.
Justification	*How might these improvements address the issues?* The current issue began when the manager forgot to rescind access by the marketing representative to this private folder. Warning the team to wait for approval before sharing the promotional materials with others is not good enough because you're reliant on the team to not share confidential information either intentionally or unintentionally. Either way by **automatically revoking access** (without the initiative of the manager) would help negate the issue in future. Furthermore, in the detailed scenario it was stated that "*Later, the representative copied a link to the marketing materials to share with a business partner during a sales call. Instead, the representative shared a link to the entire folder*". It is evident that the marketing representative had access to more than what was necessary for their role. By **restricting access to sensitive resources based on user role**, this would have reduced the amount of sensitive information made available to the public.

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.