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)	*According to the events that happened during the data leak, it is a textbook case of a problem called "Privilege Creep". Privilege creep is where one or more employees have access to more assets then they need to. Unable to follow and enforce the 'principle of least privilege' is what leads to privilege creep. In relation to this event, the business partner should NOT have the permission or ability to post this sensitive information on their social media*
Review	*NIST SP 8000-53: AC-6 => This is a NIST(National Institute of Standards and Technology) framework that is primarily about access privileges and the principle of least privilege, focused on protecting data privacy.* *This framework includes potential controls needed to improved the overall efficiency and effectiveness of least privilege.*

Recommendation(s)	*According to the framework NIST SP 8000-53:AC 6, the best controls to use would be:* *1-Regularly audit user privileges* *2-Restrict access to sensitive resources based on user role.* *3-Automatically revoke access to information after a period of time(optional in this scenario)*
Justification	*A data leak is a hefty problem for the company, for some information may greatly impact the confidentiality of data and trust the user base has in the company. This break of confidentiality can have dire consequences for the reputation that has been built up to this point. Preventing data leaks can be done if internal link sharing is restricted to those with the needed access to it along with ensuring that all access permissions are within the employee's job requirements through regular audits. A timing system should also be in place to reduce the amount of overhead for most internal and sensitive items, this system can automatically revoke privileges after a certain period of time to ensure no accidental leaks in between privilege audits.*

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.