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 is the abuse of principle of least privilege (PoLP). The manager, though unintentional, ought to have prioritized the information privacy of such an intellectual property.*
Review	NIST SP 800-53 is a publication by the National Institute of Standards and Technology (NIST) that provides a comprehensive set of security controls and guidelines for federal information systems and organizations in the United States. These controls are designed to help organizations protect their information and information systems. NIST SP 800-53: AC-6 specifically addresses the "Least Privilege" security control. This control is part of the "Access Control" (AC) family of controls within the NIST Special Publication 800-53 framework. The purpose of AC-

	6 is to ensure that individuals and processes are granted the minimum level of access or permissions necessary to perform their assigned tasks and functions.
Recommendation(s)	*The company's employees should only be given the minimum privilege to perform their duties with ease. More security measures should be implemented on the company's information security – with the use hashing and encryption on all restricted or sensitive data. Adding to that, multi-factor authentication (MFA) must be instituted on all the data, infrastructure, and devices belonging to the organization.*
Justification	*The implementation of least privilege principle shall be a massive boost to the overall security of the company's assets. Hashing and encryption is extremely vital for data governance. MFA will be there to confirm, for sure, that the information being assessed actually ends up in the hands of a trusted data custodian, owner, or steward.*

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.