Data leak worksheet - Juan Cardenas

(Determine Appropriate Data Handling Practices)

Incident summary: A customer success representative received access to a folder of internal documents from a manager. It contained files associated with a new product offering, including customer analytics and marketing materials. The manager forgot to unshare the folder. Later, the representative copied a link to the marketing materials to share with a friend during a sales call. Instead, the representative copied a share link to the entire folder. During the sales call, the business partner received the link to internal documents and posted it to their social media page.

Control	**Least privilege**
Issue(s)	*Access to the internal folder should have been limited to the representative and their manager. The customer should have gotten permission to share the marketing information before posting it to 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)	• *Automatically revoke access to information after a period of time.* • *Regularly audit user privileges.*
Justification	*A policy about setting expiration dates for share links could address situations where employees forget to manage their information. Having managers and security teams regularly audit access to team files might also keep important information secure from unauthorized users.*

Security plan snapshot

The 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 organizational 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.