Data leak worksheet

Incident summary: A data leak occurred when a customer success representative, granted access to a folder by a manager, unintentionally shared a link to internal documents during a sales call. The manager failed to revoke access to the folder, leading to unintended exposure. The customer then posted the link on social media, highlighting issues with oversight and adherence to the principle of least privilege. Recommended control enhancements include automated access reviews and user training to prevent similar incidents.

Control	Least privilege
Issue(s)	*The data leak occurred when a customer success representative, granted access to a folder by a manager, inadvertently shared a link to internal documents during a sales call. The manager forgot to unshare the folder, leading to unintended access and subsequent social media exposure. Lack of proper oversight and adherence to the principle of least privilege contributed to the incident.*
Review	*The company's security plan is aligned with the NIST Cybersecurity Framework (CSF), utilizing NIST SP 800-53 for information privacy. NIST SP 800-53: AC-6 specifically addresses access control, emphasizing the principle of least privilege.*
Recommendation(s)	• *Implement automated folder access review processes to promptly identify and rectify unintended sharing.* • *Require multi-factor authentication for accessing sensitive folders and documents.* • *Strengthen the monitoring of user activities within sensitive folders.*
Justification	*The recommended control enhancements address the root causes*

	identified in the incident. Automated reviews ensure swift response to access issues, minimizing the window of vulnerability. User training promotes a culture of vigilance, reducing the likelihood of inadvertent data exposure. Together, these measures strengthen the company's information privacy framework, aligning with the principles of the NIST SP 800-53: AC-6 control category.

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.