

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)	<i>What factors contributed to the information leak?</i> <i>The internals-only folder had no privilege policies because the sales manager gave their team full access and the employee could share it with a business partner. The manager also disregarded information privacy by not revoking access to the folder after the meeting.</i>
Review	<i>What does NIST SP 800-53: AC-6 address?</i> <i>AC-6 focuses on the least privilege principle. Roles should be enforced as necessary with only minimal access and authorization required to complete a task or function. This prevents roles from operating at a higher privilege than allowed to protect sensitive information.</i>

Recommendation(s)	<p><i>How might the principle of least privilege be improved at the company?</i></p> <p><i>Based on AC-6 suggestions restricting access to sensitive resources based on user role and automatically revoking access to information after a period would improve information security at the company.</i></p>
Justification	<p><i>How might these improvements address the issues?</i></p> <p><i>The data leak was caused by unwanted users accessing sensitive information because of a lack of user privilege restriction. Restricting users' access to information based on their role would stop employees from sharing outside the need-to-know-basis group. Automatically revoking access to information after some time would allow managers to share internals-only information with employees without compromising data privacy.</i></p>

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: <i>Data security</i>	PR.DS-5: <i>Protections against data leaks.</i>	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 the least privilege. The intention is to prevent users from operating at privilege levels higher than necessary to accomplish business objectives.
	Control enhancements: <ul style="list-style-type: none">● 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.