

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)	<p><i>What factors contributed to the information leak?</i></p> <ol style="list-style-type: none"><i>1. The sales manager initially shared access to internal documents with their team without revoking access after the meeting.</i><i>2. The sales representative accidentally shared a link to the internal folder with a business partner during a video call.</i><i>3. The business partner mistakenly posted the link on their company's social media page, assuming it was promotional materials.</i>
Review	<p><i>What does NIST SP 800-53: AC-6 address?</i></p> <p><i>The issue of managing information system accounts, including the principle of least privilege. It emphasizes that access to resources and actions should be restricted to only what is necessary for authorized users to accomplish their tasks.</i></p>

Recommendation(s)	<p><i>How might the principle of least privilege be improved at the company?</i></p> <ol style="list-style-type: none"> <i>1. Implement access controls: Define specific access levels and permissions for different users based on their roles and responsibilities.</i> <i>2. Regularly review and update permissions: Conduct periodic reviews of user access rights and adjust them as needed. Remove unnecessary access permissions.</i> <i>3. Use role-based access control (RBAC): Implement RBAC to assign permissions based on predefined roles, ensuring that users have access only to what is essential for their job functions.</i> <i>4. Educate employees: Provide training to employees about the importance of least privilege and the proper handling of sensitive information.</i>
Justification	<p><i>How might these improvements address the issues?</i></p> <p><i>By implementing the principle of least privilege and the recommended measures, the company can reduce the risk of unauthorized access to sensitive information.</i></p> <p><i>Users will only have access to the resources and data necessary for their roles, minimizing the potential for accidental data leaks.</i></p> <p><i>Regular reviews and education will help maintain a strong security posture and prevent similar incidents in the future.</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 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: <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.