

# 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>The data leak occurred because a sales manager shared access to an internal folder but did not revoke access after the meeting. A sales representative mistakenly shared the entire folder instead of just the promotional materials. The business partner, unaware of the confidentiality, posted the link publicly.</i>
Review	<i>NIST SP 800-53: AC-6 focuses on enforcing the principle of least privilege, ensuring users have only the necessary access to perform their tasks. It includes recommendations such as restricting access based on roles, revoking access automatically after a set time, logging user activities, and conducting regular audits to prevent unauthorized data exposure.</i>

<b>Recommendation(s)</b>	<p>Implement <b>role-based access control (RBAC)</b> to ensure employees can only access the specific data they need.</p> <p>Configure <b>automatic access expiration</b> for shared folders to revoke access after a set period, reducing the risk of unintentional leaks.</p>
<b>Justification</b>	<p>Role-based access control would have prevented the sales representative from accessing internal documents beyond their role's necessity. Automatic access expiration would have ensured that employees lost access to confidential data after the meeting, minimizing the chance of accidental sharing. These measures would significantly enhance data security and privacy.</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)
<b>Protect</b>	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	<b>Least Privilege</b>
	<p>Control:</p> <p>Only the minimal access and authorization required to complete a task or function should be provided to users.</p>
	<p>Discussion:</p> <p>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.</p>
	<p>Control enhancements:</p> <ul style="list-style-type: none"><li>● Restrict access to sensitive resources based on user role.</li><li>● Automatically revoke access to information after a period of time.</li><li>● Keep activity logs of provisioned user accounts.</li><li>● Regularly audit user privileges.</li></ul>

**Note:** In the category of access controls, SP 800-53 lists least privilege sixth, i.e. AC-6.