

# 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 principle of least privilege was not followed during this incident. The customer success representative should not have had access to the entire folder, only to the specific documents that they needed for the meeting.</i>
Review	<i>NIST 800-53: AC-6 addresses the principle of least privilege. It describes what least privilege is, how it should be implemented, and ways to improve the effectiveness of the control.</i>
Recommendation(s)	<ul style="list-style-type: none"><li>• Restrict access to sensitive resources based on user role.</li><li>• Regularly audit user privileges.</li></ul>
Justification	<i>Restricting access can easily prevent human error by never putting an employee in a position where they can accidentally share information that is</i>

	<i>confidential. This can be reinforced by regular audits of user privileges to reduce the likelihood of a data leak of sensitive information.</i>
--	--

# 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"><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.