

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>There are several factors contributing to the data leak, one would be due to unrevoked access to sensitive data. The sales manager was the primary cause of the data leak since confidential data must be secured and only authorized personnel can access the information.</i></p> <p><i>Another factor contributing to the data leak would be Human error. It is the most common cause of any data leak, the sales representative accidentally shared the link of the sensitive data instead of the intended materials.</i></p>
Review	<p><i>NIST SP 800-53: AC-6 is a framework that addresses the access control of information in an organization. The AC-6 category is titled “Least Privilege” and it focuses on restricting access rights for individuals to the minimum levels necessary to perform their job functions. The goal is to prevent users</i></p>

	<i>or processes from having unnecessary access to sensitive information or system resources, thereby reducing the risk of unauthorized actions and potential security breaches.</i>
Recommendation(s)	<p><i>Implement a regular access review process to ensure that team members only have access to the information necessary for their roles.</i></p> <p><i>After the meeting, the sales manager should have promptly revoked access to the internal folder, limiting continued access to only those who genuinely need it.</i></p>
Justification	<i>The initial sharing of the internal folder with the entire team might indicate a lack of proper access controls. By implementing role-based access controls, it will ensure that only individuals with a legitimate need can access 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">● 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.