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)	*The following elements led to the leak of internal-only information:* - *The folder of internal-only documents contained information that should not be shared with the public, along with promotional materials that would eventually be shared with the public. These promotional materials should have been separated to begin with* - *The manager did not revoke access to the internal folder after the meeting, and gave the staff permission to access the promotional materials for distribution, which is fine under normal circumstances, however the internal-only documents were still accessible* - *Instead of manually distributing the promotional documents to the appropriate staff members, the manager decided to leave the responsibility of ensuring they send the right documents, increasing the risk of information leak since now many individuals had access*

	- *One staff member made an error by sending the internal-only information that had not yet been announced to one of their business partners, who assumed the information they received was ready to be shown to the public.*
Review	*NIST SP 800-53: AC-6 addresses the following:* *Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.* *Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.*
Recommendation(s)	*The following are ways the principle of least privilege could be improved within the company:* - *Documentation that is not intended for public knowledge should be separated from materials that are intended for promotional or public distribution. Separate folders can be used, or even sub-folders with clear labeling* - *Permissions could be revised so that only authorized users or groups can access the internal-only documents. If these internal-only documents ever needed to be accessed by new groups or*

	individuals, the permissions could be revised, or management can manually send them to the appropriate staff members. - *The manager in charge of the meeting could have manually extracted the promotional materials without ever giving access to the internal-only documents to avoid giving everyone non-essential access to the files. The manager could then send a link or e-mail to the promotional materials without ever giving direct access to the other documents in the folder.* - *The manager could also have revoked permissions to access the folder after the meeting to ensure nobody can erroneously send the wrong document*
Justification	*These improvements may address the issue through the following:* - *Limiting access to sensitive documents prevents anyone from making the mistake of sending the incorrect document to business partners who should never have access, since these documents contained the company's agenda and private information* - *Giving the least privilege possible means that there will be no confusion as to what can and cannot be shared with business partners, and nobody needs to gain permission from management, since permissions are already set through the system* - *These improvements eliminate the risk of human error when dealing with sensitive information*

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: *Data security*	PR.DS-5: *Protections against data leaks*.	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: • 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.