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)	*What factors contributed to the information leak?* *The sales manager shared access to an internal folder containing sensitive documents with their entire team, rather than restricting access to only those who required it. Additionally, the lack of timely revocation of access further exacerbated the risk by allowing unauthorized individuals to retain access to the confidential information.*
Review	*What does NIST SP 800-53: AC-6 address?* *It addresses the management of access to information systems and associated assets. It focuses on establishing access controls, such as authentication mechanisms and access permissions, to ensure that only*

	authorized users are granted access to resources and that unauthorized access attempts are prevented or detected. The goal is to protect the confidentiality, integrity, and availability of information and resources within an organization's IT infrastructure.
Recommendation(s)	*How might the principle of least privilege be improved at the company?* *To improve the principle of least privilege at the company, access permissions should be regularly reviewed and adjusted based on employees' roles and responsibilities. Implementing role-based access controls (RBAC) can streamline this process by assigning permissions based on predefined job functions, ensuring that individuals have access only to the resources necessary for their specific tasks. Additionally, implementing automated access control mechanisms and monitoring tools can help enforce least privilege principles in real-time, reducing the risk of unauthorized access.*
Justification	*How might these improvements address the issues?* *Implementing regular reviews and adjustments of access permissions based on roles and responsibilities ensures that individuals only have access to the information necessary for their tasks, reducing the likelihood of unauthorized access. Role-based access controls streamline this process, making it easier to enforce the principle of least privilege across the organization. Automated access control mechanisms and monitoring tools provide real-time visibility into access activities, enabling prompt detection and mitigation of any unauthorized access attempts, thereby enhancing overall data security and mitigating the risk of information leaks.*

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.