Data leak worksheet

Incident summary: An employee accidentally shared a private internal business plan with an external business partner during a sales meeting, causing the document to be exposed on social media. According to the inquiry, this breach happened as a consequence of workers who did not need such access for their jobs gaining unlawful access to sensitive data due to a failure to follow the principle of least privilege.

Control	**Least privilege**
Issue(s)	What factors contributed to the information leak? Some factors that contributed to the information was; **Lack of adherence to the principle of least privilege**: the employee had access to documents that was not necessary for their role and also access rights enabled the accidental sharing of sensitive documents during a sales meeting. **Inadequate access control:** to me I think that the organization did not implement or enforce role based access control (RBAC), and there were no limitations on the dissemination of private data to unapproved parties. **Human error**: The employee was unaware of the document's sensitivity and ramifications. **Insufficient employee training and awareness:** lack of regular training on company policies, data handling best practices. Company should ensure that employees are well trained and aware of cybersecurity principles.
Review	What does NIST SP 800-53: AC-6 address? It addresses how organizations can protect their data privacy by implementing the principle of least

	privilege. It requires that devices, processes or users have the bare minimum of access rights required to carry out duties to perform their assigned task.
Recommendation(s)	How might the principle of least privilege be improved at the company? ● Strengthen access controls. ● Data classification and labeling. ● Enhanced employee training. ● Data sharing and collaboration policies. ● Incident response plan enhancement.
Justification	Data leaks can be avoided if sharing links to internal files are limited to workers only. Additionally, mandating that management and security teams conduct routine audits of team file access would assist reduce the vulnerability of private 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.