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.

INCIDENT ANALYSIS	
Control	**Least privilege**
Issue(s) *What factors contributed to the information leak?*	*A sales manager shared access to an internal-only folder to their team for a meeting. It contained upcoming product details and related research work.* *The access to the folder was not revoked after the meeting.* *A new sales team member accidentally shared the link to this folder to a business partner thinking it to be a link to promotional materials and the business partner, without checking the link, posted the link on their social media page.* *Key Security Problems :* • *Breakdown in access controls and lack of verification before external sharing*

INCIDENT ANALYSIS	
	• *Inadequate enforcement of access control policies* • *Lack of automatic deprovisioning mechanisms* • *Insufficient employee awareness of data classification*
Review *What does NIST SP 800-53: AC-6 address?*	*NIST SP 800 - 53: AC-6* *It defines **controls for enforcing the principle of least privilege**. It provides a recommendation of control implementation with respect to minimum or need basis access.* • ***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.***
Recommendation(s) *How might the principle of least privilege be improved at the company?*	*It is clear that there has been a lapse in implementing effectively the least access privilege control.* *Recommendation:* • *Any privilege provided must be **given only on need basis*** • *Once the needed job is done **access** must be **revoked*** • *Access can be revoked **automatically** to confidential information **after a period of time*** • *All **confidential files** can be **password protected** to ensure that even after any link is shared accidentally also, file cannot be accessed without password* • *Make **employees** accountable for the **resources** shared to them* • *Maintain **access logs** for confidential / restricted information* • ***Access / credential sharing** must be prohibited*

INCIDENT ANALYSIS	
	• ***Communicating*** *to* ***business partners*** *to treat any resources shared with care even if it is promotional material, it must be checked and then publicly shared* • ***Ownership rights*** *must be granted with utmost care* • ***Employees must be trained*** *to know that confidential / restricted information must be handled with care, responsibility and accountability* • ***Access reviews*** • ***Periodic audits*** *of* ***shared resources***
Justification *How might these improvements address the issues?*	• *Many recommendations are as per the NIST SP 800 - 53: AC-6 which are self explanatory in nature* • *Password protection is a simple way to prevent any files from being read even if the folder link is available* • *Access logs allow security teams to trace and track privileges as they were granted* • *When employees are held accountable & receive training related to privileges they have and how to act responsibly with information, then they tend to access and share access to those resources with caution. This helps in prevention of privilege creep.* • *Periodic audit helps* ○ *Ensuring users don't retain access beyond their responsibilities.*

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.