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 manager of the CSR neglected to revoke access to the sensitive data. As a consequence, the CSR during a call with a customer shared the data by accident. Instead of just sharing the relevant information, the CSR shared the entire folder with the customer leading to the customer posting the information on their social media.*
Review	*NIST SP 800-53: AC-6 addresses the principle of least privilege security measure. This ensures that data only gets accessed by people who need permission to do their day to day functions and makes risking sensitive data much less likely. This principle, if implemented prior to this incident, would have prevented the CSR from having access to the sensitive data therefore they would not have leaked it to their customer by accident.*

Recommendation(s)	*One control enhancement to implement that would make principle of least privilege more impactful would be to make sure access to sensitive data is revoked if temporarily made available for a employee to complete a business function. Another recommendation would be to log and audit user privileges and accounts to ensure no user has access to data that is outside of their roles base functions, keeping data secure.*
Justification	*Justification for my recommendations are as follows:* *In the given incident, having temporary access to sensitive data for an employee to review and process for their day to day functions is necessary. That information is impactful for the employee to do their job but they do not need full access to that data on a 24/7 basis and as a result of no temporary access measures in place, lead to a leak of data. Logging and auditing user privileges and accounts regularly would also see and solve potential threats in which users are given temporary access to more sensitive data and not have that privilege revoked after necessary functions have been completed.*

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.