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 sales manager shared the access to the folder with the team and he/she didn't revoke the access to the internal folder. The business partner shouldn't have been given permission to share on social media the link the sale representative gave to him.
Review	NIST SP 800-53: AC-6 is a set of guidelines that address to an action that aim to protect organizations from data leaks by implementing least privileges. It also suggest to enhance the control to improve the security of important files.
Recommendation(s)	• Restrict access to data in base of the user role. • Regulars checks for users' privileges.

Justification	• By restricting the access to data, we avoid to let people, with lack of knowledge on how to use important files, make mistakes on leaking them, modify or even delete them. • Keeping a correct users' privileges avoid security breaches from older users that shouldn't have those privileges or older users not deleted.