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 team was only supposed to have access to the internal folder for the duration of the meeting, however access was not revoked. The sales manager, knowing the sales team was not supposed to have access to the material outside the meeting, decided to not revoke permissions, but instead trust a verbal warning instead. This led to the sales team leaking information to their business partner due to them forgetting about the warning, leading to the folder being leaked.*

Review	*The NIST SP 800-53: AC-6 addresses that only minimal access and authorization should be granted to a user to perform a task or role. Access and authorization should only be granted as necessary to prevent users from having too much privilege for the tasks or roles they were assigned.*
Recommendation(s)	• *Restrict access to sensitive resources based on user role.* • *Regularly audit user privileges.*
Justification	*These improvements can help prevent data leaks by ensuring that internal files are only shared between employees. Performing regular privilege audits on users can limit exposure on sensitive information.*