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 should have restricted access to the sensitive company assets as soon as the meeting was over as the access was no longer needed for jobs functions for those users.*
Review	*Least privilege (*NIST SP 800-53: AC 6) should be upheld to ensure that no sensitive company assets/data are leaked to the public even if non-maliciously.
Recommendation(s)	*I would recommend user training for all managers to ensure and uphold the principle of least privilege based on user role and reporting.* *There should be logs and regular audits to ensure all user roles and security groups are up to date and uphold the principle of least privilege.*

Justification	*Data/asset leaks can be prevented if shared links to internal files are restricted to the correct users/groups.* *Requiring managers to be trained on the principle and its importance leads to a culture of privacy and information security. Managers and security teams regularly* *auditing access would help limit the exposure of sensitive information.*