Data leak report

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 factors that contributed to this incident are:* ● The manager after sharing internal-only files with his team did not revoke access to the files after the meeting. ● The sales team member had access to the internal folder for too long which allowed them to forget the warning to not share the files. ● Human error as the member accidentally shared the link to the internal folder with an unauthorised person. ● The business partner who is an unauthorised user was not prompted for any authentication before being allowed access to view and even share the files. *These issues are a mix of human error (which is a major vulnerability), lack of proper access controls and poor Identity and Access management procedures.*

Review	*NIST SP 800-53: AC-6 addresses the principle of Least Priviledge. This states that only the minimum access to a resource should be granted to a user for the user to complete a certain task.* 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.
Recommendation(s)	*I recommend that in order for us to implement the PoLP, some controls must be put in place:* ● 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.