Data Leak Assessment

Incident Summary

A customer success representative received access to a folder of internal documents from a manager. It contained files associated with a new product offering, including customer analytics and marketing materials. The manager forgot to un-share the folder. Later, the representative copied a link to the marketing materials to share with a customer during a sales call. Instead, the representative shared a link to the entire folder. During the sales call, the customer received the link to internal documents and posted it to their social media page.

Assessment

Control	Least Privilege
Issue(s)	The manager granted unnecessary access to internal documents and failed to revoke it. The representative, unaware of the extent of access, inadvertently shared the complete folder.
Review	NIST SP 800-53: AC-6 emphasizes limiting user access to only what's essential for their tasks. It suggests controls such as restricting access based on roles and regularly auditing privileges.
Recommendation(s)	Restrict access to sensitive resources based on user role. Regularly audit user privileges.
Justification	By assigning access based on roles, employees will only access information relevant to their tasks, reducing potential leaks. Regular audits by managers and security teams will catch any unwarranted access, further reducing exposure risks.