M.Kesten, March ’24.

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 leak happened because the manager didn’t remove access to secret files after a meeting and also didn’t make the rules clear. The team member shared a link to these files, which led to leak of information.
Review	NIST SP 800-53: AC-6 focuses on the principle of least privilege, ensuring that users have only access necessary to perform their task. It’s minimizing potential exposure of sensitive information and emphasize strict access controls and regular reviews of user permissions to protect against unauthorized access and data leaks.
Recommendation(s)	1. **Restrict access to sensitive resources based on user role**: Ensuring that acces to sensitive data is based on user's role prevents unauthorized sharing by limiting access to those who truly need it for their task. 2. **Automatically revoke access to information after a period of time**:

	Implementing system that automatically revokes access rights to sensitive information after a set period can prevent the data leak by ensuring that access is only temporary.
Justification	By restricting access based on user roles and automatically revoking access over time, we significantly reduce the risk of accidental or unauthorized sharing.