### **Rhiannon Goebel | 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 sales manager did not properly limit the availability of the data (either by an expiration to access the link or a limit on access to only the sales team even if external individuals had the link). The sales team member did not ensure the proper link was shared, did not implement access limitations to the confidential files, and should not have given permission for the business partners to share the information on social media.* |
| **Review** | *NIST SP 800-53: AC-6 addresses how implementing least privilege access to data can help organizations protect their data privacy, and best practices to do so.* |
| **Recommendation(s)** | *Restricting access to data and files based on individuals’ role and if they are internal to the company, setting data access time limitations for those who aren’t owners of the data, and performing regular audits on user data access privileges.* |
| **Justification** | *Restricting access to the files would have prevented the business partner from being able to access the files even if they had the link. Requiring regular audits of access privileges would have flagged the lack of limitations on access to the data and prevented the exposure of sensitive data.* |