# 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)** | Too many people had access to the information. The principle of least privilege was not applied correctly and therefore over time, more and more people had access to the data. |
| **Review** | *What does NIST SP 800-53: AC-6 address?*<br>It addresses the principle of least privilege, it gives users only the minimum access to resources that they need to complete normal business operations. |
| **Recommendation(s)** | *How might the principle of least privilege be improved at the company?*<br>- Restrict access to sensitive resources based on user role.<br>- Regularly audit user privileges. |
| **Justification** | *How might these improvements address the issues?*<br>Data leaks can be prevented if shared links to internal files are restricted to employees only. Also, requiring managers and security teams to regularly |

| | |
|---|---|
| | audit access to team files would help limit the exposure of sensitive information. |