Data Handling Practices

**Scenario:**

**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.

**Evaluation of details:**

**Issue:** The data is not segregated based on the complexities and combined Internal and Confidential in the same folder. The access was given to the entire folder instead of specific files required for the meeting. Before sharing the information either the Business partner or sales representative hasn’t checked the folder before uploading it which should not be as security is everyone’s responsibility.

**Review:** NIST SP 800-53: AC-6 addresses how an organization can protect its data privacy by implementing least privilege. It also suggests control enhancements to improve the effectiveness of least privilege.

**Recommendations:**

* Segregate the files based on the asset classification.
* Restrict the access based on user role using least privilege.
* User Training on how to handle data.
* Regularly audit user privileges.
* Monitor the files before upload and warn incase of any non-Internal or non-public data classified is being uploaded in portals.

Reference:

NIST 800-53 AC-6 PR.DS-5: *Protections against data leaks.*