Data Leak Worksheet

# Issue(s)

The manager mistakenly granted access to an entire internal folder instead of individual files. The customer success representative, unaware of the scope, shared the full folder link with an external partner, who then posted the confidential information publicly.

# Review

NIST SP 800-53: AC-6 emphasizes enforcing the principle of least privilege by ensuring users only have access to the resources necessary for their roles. It highlights the importance of reviewing, limiting, and controlling permissions to reduce accidental or malicious data exposure.

# Recommendation(s)

1. AC-6 (1): Least Privilege | Authorize Access to Security Functions – Ensure that only authorized personnel can access and share security-sensitive or internal files.  
2. AC-6 (5): Least Privilege | Privileged Access by Role – Restrict access based on predefined roles to ensure employees only see information relevant to their responsibilities.

# Justification

By restricting access based on role and ensuring only authorized users can share sensitive content, the risk of accidental data leaks is minimized. These controls would have limited the representative’s access and ability to share confidential documents, preventing the leak.