Data Leak Assessment, Least Privilege Review

1. Introduction

Information privacy is critical to protecting intellectual property and sensitive business data. This report documents an internal review of a data leak incident caused by improper access controls and violations of the principle of least privilege. The objective of this assessment is to identify contributing factors, evaluate existing controls, and recommend improvements aligned with NIST SP 800-53 AC-6.

2. Incident Summary

During a sales meeting, a manager shared access to an internal only folder containing confidential product information, customer analytics, and promotional materials. Access to the folder was not revoked after the meeting. During a later sales call, an employee accidentally shared the entire internal folder with an external business partner, who subsequently posted the link publicly on social media.

---

3. Control Review: Least Privilege (NIST SP 800-53 AC-6)

NIST SP 800-53 AC-6 addresses the principle of least privilege, which requires users to be granted only the minimum access necessary to perform their job functions. The control emphasizes role-based access, limiting authorization scope, and preventing privilege creep. Proper implementation reduces the risk of unauthorized or accidental data exposure.

4. Identified Issues

The data leak occurred because access to sensitive internal documents was broadly shared and not technically restricted. The organization relied on verbal warnings

instead of enforcing access controls. As a result, employees retained unnecessary access and were able to unintentionally share confidential information externally.

5. Recommendations

To improve enforcement of least privilege and prevent future data leaks, the following control enhancements are recommended:

- Automatically revoke access to shared folders after a defined time period.
- Restrict access to sensitive internal folders based on user roles and limit external sharing to approved files only.

6. Justification

These improvements reduce the likelihood of accidental data exposure by limiting both the scope and duration of access to sensitive information. Enforcing role-based access and automatic expiration of permissions ensures confidential documents are only accessible to authorized users, strengthening information privacy and adherence to least privilege principles.

7. Visual Summary

(Insert the color-coded table image here)
Figure 1: Least Privilege Assessment and Control Improvements (NIST SP 800-53 AC-6)

8. Conclusion

This assessment highlights how insufficient enforcement of least privilege can lead to data leaks, even in the absence of malicious intent. Implementing technical access controls aligned with NIST SP 800-53 AC-6 strengthens information privacy, reduces human error, and improves the organization's overall data protection posture.

Prepared by: **Sambou Kamissoko**
LinkedIn: https://www.linkedin.com/in/sambouk/