Cybersecurity Incident Report: Data Leak

1. Incident Summary

- **Type of Incident:**
  Data leak due to improper sharing of internal resources.
- **Incident Description:**
  During an internal meeting, a sales manager shared access to a folder containing internal documents about a new product not yet publicly announced. Although the manager advised the team not to share the materials until they received approval, they did not revoke access to the folder after the meeting. Later, a member of the sales team accidentally shared a link to the internal folder with a business partner during a video call. The partner, assuming it was promotional material, posted the link on their company's social media page, thereby exposing confidential information.

2. Incident Analysis

- Access Management Error:
  Access to the internal folder was not properly restricted. After the meeting, permissions were not revoked, allowing the sales team ongoing access to sensitive information. Due to the lack of additional controls, a sales team member inadvertently shared the wrong link with the business partner.
- Social Media Exposure:
  The business partner posted the link to the internal folder on their social media page, assuming it contained promotional materials approved for distribution. This resulted in a public leak of sensitive information, including customer analysis and product details.

3. Affected Control: Principle of Least Privilege

The principle of least privilege was not adequately enforced. The sales team was given unrestricted access without temporary or role-based limitations, which allowed the information to be accidentally shared with a third party.

Identified Issues:

- Lack of Restrictions:
  Access to the folder was not properly restricted after the meeting.
- Inappropriate Permissions for Third Parties:
  There was no clear policy prohibiting the sharing of promotional information without prior approval.

4. Recommendations for Improvement

- Role-Based Access Restrictions:
  Implement controls that limit access to sensitive information only to users who need it for their specific roles.
- Periodic Audits:
  Regularly audit user access privileges to identify and correct any excess permissions.
- Automatic Access Revocation:
  Configure systems to automatically revoke access to sensitive folders after a specific period or once the task for which access was granted has been completed.
- Training and Awareness:
  Ensure all employees understand security policies, especially regarding document sharing and the use of third-party platforms.

5. Security Plan: NIST Framework Implementation

The NIST Cybersecurity Framework (CSF) is used to organize information and protect data within a company. Under this framework, the AC-6 Least Privilege control is designed to ensure that users only have the necessary permissions to perform their jobs, minimizing exposure to sensitive data.

Recommended Controls:

- Control AC-6: Least Privilege
  Defines that users should only have access to the resources necessary to perform their work, minimizing the exposure of sensitive information.
- Control Enhancements:
  - Restrict access to sensitive resources based on user roles.
  - Automatically revoke access to information after a set period.
  - Maintain detailed logs of user account activity and periodically audit these logs.

6. Conclusion

This incident highlights the need for stricter security controls, such as the principle of least privilege and continuous auditing of access to information. Implementing the provided recommendations, along with a security plan based on the NIST framework, will help prevent future data leaks and protect the organization’s sensitive information.