### **Data leak worksheet**

### **Incident Summary**

A sales manager shared access to an internal-only folder containing confidential business plans, customer analytics, and promotional materials during a meeting. After the meeting, the manager did not revoke access to the folder. A sales representative, intending to share promotional materials with a business partner, mistakenly shared the link to the entire internal folder. The business partner then posted the link on social media, believing it to be public content.

### **Issue(s): What factors contributed to the information leak?**

1. **Failure to Follow Least Privilege:** The sales team was given access to internal documents they did not need for their role.
2. **Lack of Access Revocation:** The manager did not revoke access after the meeting, leaving the documents exposed.
3. **Human Error:** The sales representative forgot the warning and shared the incorrect link.
4. **Unrestricted Link Sharing:** The folder link was not restricted to internal use, allowing external access.
5. **No Data Leak Prevention (DLP) Controls:** There were no automated systems to prevent accidental external sharing.

### **Review: What does NIST SP 800-53: AC-6 address?**

NIST SP 800-53: AC-6 defines the principle of **Least Privilege**, ensuring users have only the minimal level of access necessary to perform their tasks. It aims to:

* Restrict access to sensitive resources based on user roles.
* Automatically revoke access after a set period.
* Maintain activity logs of user access.
* Regularly audit user privileges.

This control helps prevent unauthorized access and limits the risk of data exposure due to mismanagement of permissions.

### **Recommendation(s): How might the principle of least privilege be improved at the company?**

1. **Implement Role-Based Access Control (RBAC):**
   1. Restrict access to confidential folders based on specific roles. Only necessary personnel should have access to sensitive information.
2. **Enforce Automatic Access Revocation:**
   1. Configure the system to revoke access to shared folders after a predefined time, ensuring temporary access is not left open indefinitely.
3. **Stricter Link-Sharing Policies:**
   1. Require additional authentication for external sharing and limit the ability to create unrestricted links.
4. **Data Loss Prevention (DLP) Tools:**
   1. Deploy DLP solutions to monitor and prevent unauthorized sharing of sensitive documents.
5. **Employee Training:**
   1. Conduct regular training to reinforce the importance of data security and awareness of best practices.

### **Justification: How might these improvements address the issues?**

* **Role-Based Access Control (RBAC):** Ensures only authorized personnel can access sensitive documents, reducing the risk of accidental exposure.
* **Automatic Access Revocation:** Prevents prolonged access to sensitive information, mitigating the risk of forgotten permissions.
* **Stricter Link-Sharing Policies:** Enhances control over how documents are shared externally, ensuring only appropriate materials are disseminated.
* **Data Loss Prevention Tools:** Act as an automated safeguard against accidental data leaks by detecting and blocking unauthorized sharing.
* **Employee Training:** Increases awareness of data security practices, reducing human error and reinforcing the importance of proper data handling.

These improvements align with NIST SP 800-53 guidelines, enhancing data security and ensuring the principle of least privilege is effectively implemented across the organization.