### **Data leak worksheet**

**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.

| **Control** | **Least privilege** | | |
| --- | --- | --- | --- |
| **Issue(s)** | *What factors contributed to the information leak?*  *During a Sales Meeting, the Sales Manager was able to access the internal-only folder and found files associated with a New product as well that was yet to be launched, the Manager forewarned the sales team not to share this New product info with others and ask for his approval before sharing the info. Here the Manager should have revoked access to sales regarding New product info except to the people who were working on the product.*  *Later, During a video call , a member of the sales team shared the New Product info instead of promotional material to an external business partner and the Business Partner shared the link as such assuming that it was the link to promotional material and that’s how the data leak occurred. Here the Sales Representative should have asked for the Manager’s approval , as the manager forewarned about this scenario.* | | |
| **Review** | *What does NIST SP 800-53: AC-6 address?*  *NIST SP 800-53 AC-6 is about Least Privilege Access and LPA address the issue of accidental leak of sensitive and confidential information by an unauthorized user / user who shouldn’t have the access to that particular information* | | |
| **Recommendation(s)** | *How might the principle of least privilege be improved at the company?*  *It Improves the data from*   * *Accidental/ unintentional data leak* * *Limited access to the users so that the data cannot be manipulated/ destroyed* * *Data theft* * *Activity log will help during investigation if a potential data leak has occurred* | | |
| **Justification** | *How might these improvements address the issues?* | | |

### **Security plan snapshot**

The NIST Cybersecurity Framework (CSF) uses a hierarchical, tree-like structure to organize information. From left to right, it describes a broad security function, then becomes more specific as it branches out to a category, subcategory, and individual security controls.

| **Function** | **Category** | **Subcategory** | **Reference(s)** |
| --- | --- | --- | --- |
| **Protect** | PR.DS: *Data security* | PR.DS-5: *Protections against data leaks.* | NIST SP 800-53: AC-6 |

In this example, the implemented controls that are used by the manufacturer to protect against data leaks are defined in NIST SP 800-53—a set of guidelines for securing the privacy of information systems.

**Note:** References are commonly hyperlinked to the guidelines or regulations they relate to. This makes it easy to learn more about how a particular control should be implemented. It's common to find multiple links to different sources in the references columns.

### **NIST SP 800-53: AC-6**

NIST developed SP 800-53 to provide businesses with a customizable information privacy plan. It's a comprehensive resource that describes a wide range of control categories. Each control provides a few key pieces of information:

* **Control:** A definition of the security control.
* **Discussion:** A description of how the control should be implemented.
* **Control enhancements:** A list of suggestions to improve the effectiveness of the control.

| **AC-6** | **Least Privilege** |
| --- | --- |
| Control:  Only the minimal access and authorization required to complete a task or function should be provided to users. |
| Discussion:  Processes, user accounts, and roles should be enforced as necessary to achieve least privilege. The intention is to prevent a user from operating at privilege levels higher than what is necessary to accomplish business objectives. |
| Control enhancements:   * Restrict access to sensitive resources based on user role. * Automatically revoke access to information after a period of time. * Keep activity logs of provisioned user accounts. * Regularly audit user privileges. |

**Note:** In the category of access controls, SP 800-53 lists least privilege sixth, i.e. AC-6.