### **Data leak worksheet**

| **Control** | **Least privilege** | | |
| --- | --- | --- | --- |
| **Issue(s)** | *The information leak occurred due to improper access control, failure to revoke permissions after the meeting, and lack of clear communication regarding sensitive files. Additionally, the sales representative's oversight in verifying the link before sharing contributed to the mishap.* | | |
| **Review** | *NIST SP 800-53: AC-6 describes the need to enforce the principle of least privilege, restricting user’s access to only the resources needed for their job. This reduces the risk of unauthorized access or accidental information leakage.* | | |
| **Recommendation(s)** | *Role-based access controls should be implemented. Additionally, automatic expiration of links should also be in place, while also training employees on how to securely handle confidential materials.* | | |
| **Justification** | *The risk of accidental sharing will be minimized by limiting access and the introduction of automated safeguards. Training employees further reinforces awareness.* | | |

### **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.