### **Data leak worksheet**

**Incident summary:** During a team meeting, I shared a folder containing internal-use documents related to a new, unreleased product. These documents included customer insights and draft marketing content. While I reminded the team to wait for official approval before sharing the promotional materials, I mistakenly left access to the folder open after the meeting.

Later, during a video call with a business partner, one of our sales reps forgot my warning and meant to share just the promotional content. Instead, they accidentally sent the link to the entire internal folder. The partner, thinking it was meant for public distribution, posted the link on their company's social media.

|  |  |
| --- | --- |
| **Control** | **Least privilege** |
| **Issue(s)** | *Access to the sensitive folder wasn’t properly limited. The business partner should never have had the ability to access internal documents or share them publicly.* |
| **Review** | *According to NIST SP 800-53, control AC-6 emphasizes the principle of least privilege—users should have access only to what they need for their roles. Enhancements to this control include restricting access by user role and conducting routine audits of user permissions.* |
| **Recommendation(s)** | * *Implement role-based restrictions for internal file access.* * *Conduct periodic audits to ensure user privileges are current and appropriate.* |
| **Justification** | *By tightening access to internal resources and reviewing permissions regularly, we can significantly reduce the risk of accidental data leaks.* |

### **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: Provide only the access necessary for a user to perform their job.
* Discussion: Proper access controls prevent unnecessary privilege elevation.
* Enhancements:

Limit access by role

Automatically expire access

Maintain user activity logs

Conduct regular audits

|  |  |
| --- | --- |
| **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.