# Data leak worksheet

**Incident summary:** The data leak occurred due to an oversight by the manager who forgot to unshare a folder containing internal documents, granting ongoing access to a customer success representative. The representative then mistakenly shared the link to the entire folder instead of just the intended marketing materials during a sales call.

This led to the business partner receiving unauthorized access to sensitive internal documents, which were subsequently posted on social media, compromising confidential information. Lack of proper access control and a failure to verify the link before sharing were key contributors to the leak.

| Control | Least privilege |
| --- | --- |
| **Issue(s)** | *The information leak resulted from a manager's failure to unshare a folder, inadequate access control, and a customer success representative mistakenly sharing a link to the entire folder. This lapse in link verification and oversight led to unauthorized access and public exposure of sensitive documents.* |
| **Review** | *NIST SP 800-53: AC-6 addresses **"Least Privilege"** in the context of access control. It mandates that organizations enforce the principle of least privilege, which means that users should be granted only the minimum level of access necessary to perform their job functions. This minimizes the risk of unauthorized access and potential damage from compromised accounts.* |
| **Recommendation(s)** | *To enhance least privilege, the company should implement role-based access control, conduct regular access reviews, and enforce a policy that grants only necessary permissions. Utilizing automated tools for access* |

| | |
|---|---|
| | *management and conducting user training on secure practices will also help ensure adherence to this principle and mitigate risks.* |
| **Justification** | *These improvements enhance security by restricting access through RBAC, automating expiration of shared links, enforcing link verification, increasing employee awareness, auditing file shares, and properly classifying sensitive data. Collectively, they reduce human error and prevent unauthorized 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:** 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:<br>Only the minimal access and authorization required to complete a task or function should be provided to users. |
| | Discussion:<br>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:<br>• Restrict access to sensitive resources based on user role.<br>• Automatically revoke access to information after a period of time.<br>• Keep activity logs of provisioned user accounts.<br>• Regularly audit user privileges. |

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