# 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? Following a team meeting, a sales manager failed to revoke access to a folder containing files associated with a new product that had not been publicly announced after the team no longer needed access to the folder, even though approval had not been given to share the materials with others. A sales representative later shared the link to the internal folder containing the confidential documents with a business partner without approval to share the promotional materials. Additional internal documents containing information such as customer analytics were shared as well because the representative shared the entire folder, rather than sharing only the promotional materials. The principle of least privilege was not implemented because the entire sales team was given ongoing  access to information that had not been cleared for public sharing, and a business partner was provided with more* |

| | |
|---|---|
| | *information than was needed for their job function of circulating marketing materials to customers.* |
| **Review** | *What does NIST SP 800-53: AC-6 address? NIST SP 800-53: AC-6 addresses the principle of least privilege, a security control intended to ensure users are provided only the minimal level of access and authorization required to perform their specific job functions or tasks. The intention of this control is to prevent users from operating at a level of privilege higher than what is necessary for their roles. NIST SP 800-53: AC-6 indicates that organizations should restrict access access to sensitive resources based on user role, automatically revoke access after a period of time, keep activity logs of provisioned user accounts, and regularly audit user privileges.* |
| **Recommendation(s)** | *How might the principle of least privilege be improved at the company? The principle of least privilege could be improved at the company by automatically revoking access to confidential materials at the conclusion of team meetings. Employees could also be restricted from attaching internal documents or links to folders containing internal documents to emails with recipients outside of the organization to prevent customers, vendors, and other third-parties from having access to sensitive internal information. Folders containing restricted material could also be password protected so that the files cannot be opened or read by those without authorization.* |
| **Justification** | *How might these improvements address the issues? These improvements would address the issues by preventing the employee from having ongoing access to the confidential documents after the meeting. This would prevent the employee from sharing the materials beyond the team without approval. Restricting attachments that can be sent to external email addresses would* |

| | |
|---|---|
| | *prevent the customer from receiving the confidential documents even if the employee attempted to share them. Password protecting the folder could prevent the business partner from being able to open and access the documents, even if they were mistakenly sent.* |

## 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.