

# Scenario

---

## **Review the following scenario.**

You work for an educational technology company that developed an application to help teachers automatically grade assignments. The application handles a wide range of data that it collects from academic institutions, instructors, parents, and students.

Your team was alerted to a data leak of internal business plans on social media. An investigation by the team discovered that an employee accidentally shared those confidential documents with a customer. An audit into the leak is underway to determine how similar incidents can be avoided.

A supervisor provided you with information regarding the leak. It appears that the principle of least privilege was not observed by employees at the company during a sales meeting. You have been asked to analyze the situation and find ways to prevent it from happening again.

First, you'll need to evaluate details about the incident. Then, you'll review the controls in place to prevent data leaks. Next, you'll identify ways to improve information privacy at the company. Finally, you'll justify why you think your recommendations will make data handling at the company more secure.

## 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)          | <i>Access to the internal folder was not limited to the sales team and the manager. The business partner should not have been given permission to share the promotional information to social media.</i>   |
| Review            | <i>NIST SP 800-53: AC-6 addresses how an organization can protect their data privacy by implementing least privilege. It also suggests control enhancements to improve the effectiveness of least privilege.</i>                                   |
| Recommendation(s) | <ul style="list-style-type: none"><li>● <i>Restrict access to sensitive resources based on user role.</i></li><li>● <i>Regularly audit user privileges.</i></li></ul>  |
| Justification     | <i>Data leaks can be prevented if shared links to internal files are restricted to employees only. Also, requiring managers and security teams to regularly audit access to team files would help limit the exposure of sensitive information.</i> |

# 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: <i>Data security</i> | PR.DS-5: <i>Protections against data leaks.</i> | 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: <ul style="list-style-type: none"><li>● Restrict access to sensitive resources based on user role.</li><li>● Automatically revoke access to information after a period of time.</li><li>● Keep activity logs of provisioned user accounts.</li><li>● Regularly audit user privileges.</li></ul> |

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