# Data leak worksheet

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. After reviewing this scenario just reply with "Done!" as I'll ask you questions in the next prompts about this scenario.

**Incident summary:** A sales manager shared access to a folder of internal-only documents containing sensitive information related to a new product, including customer analytics and promotional materials, during a meeting with their team. After the meeting, the manager failed to revoke access to the internal folder but did warn the team to await approval before sharing the promotional materials externally.

During a video call with a business partner, a member of the sales team overlooked the manager's warning and intended to share a link to the promotional materials for circulation among the partner's customers. Regrettably, the sales representative mistakenly shared a link to the internal folder instead. Subsequently, the business partner unknowingly posted the link on their company's social media page, assuming it was the promotional materials.

Please note that the incident involves the accidental sharing of sensitive internal documents, leading to the unintended disclosure of confidential information on a public platform.

| **Control** | **Least privilege** |
|---|---|
| **Issue(s)** | 1. *Lack of Access Restrictions: Access to the internal folder was not properly limited to the authorized individuals, including the sales team and the manager. This allowed the business partner to have access to sensitive information that they should not have been granted.*<br>2. *Insufficient Least Privilege Principle: The principle of least privilege was not observed in granting permissions to individuals. The business partner was given permissions that allowed them to access and potentially share the promotional information on social media, which was beyond the scope of their role or requirement.*<br>*Access to the internal folder was not adequately restricted, as it was not limited to the sales team and the manager. Additionally, the permissions granted to the business partner were excessive, allowing them to have access to and share the promotional information on social media, which goes against the principle of least privilege.* |
| **Review** | *NIST SP 800-53: AC-6, titled "Least Privilege," provides guidance on how organizations can safeguard data privacy by implementing the principle of least privilege. This control emphasizes the importance of restricting user access rights to the minimum necessary privileges required to perform their job functions effectively. By adhering to the least privilege principle, organizations can mitigate the risk of unauthorized access to sensitive data. Furthermore, NIST SP 800-53: AC-6 suggests additional control enhancements to enhance the effectiveness of least privilege. These* |

| | |
|---|---|
| | *enhancements may include implementing role-based access controls (RBAC), conducting regular access reviews, employing strong authentication mechanisms, and establishing robust user provisioning and deprovisioning processes. By incorporating these control enhancements, organizations can further strengthen their data privacy measures and reduce the likelihood of data leaks or unauthorized access incidents.*<br>*Overall, NIST SP 800-53: AC-6 provides a comprehensive framework for organizations to protect data privacy through the implementation of least privilege and related control enhancements.* |
| **Recommendation(s)** | ● *Restrict access to sensitive resources based on user role: Implement a robust role-based access control (RBAC) system to enforce the principle of least privilege. This involves defining distinct user roles within the organization and assigning access privileges based on job responsibilities and the need to access specific resources. By aligning access permissions with user roles, the organization can limit unnecessary access to sensitive resources, reducing the potential for accidental data leaks or unauthorized disclosures.*<br>● *Regularly audit user privileges: Conduct periodic audits of user privileges to ensure they are aligned with the principle of least privilege. These audits should involve reviewing access rights assigned to each user, comparing them against their current job functions and responsibilities, and identifying any discrepancies or excessive permissions. By performing regular audits, the organization can identify and rectify any instances of over-privileged access, mitigating the risk of data leaks caused by inappropriate or outdated user privileges.*<br>*By implementing these recommendations, the organization can strengthen its data handling practices, enforce the principle of least privilege, and proactively mitigate the risk of data leaks and unauthorized access incidents.* |
| **Justification** | *Implementing restrictions on shared links to internal files, limiting access to employees only, is a crucial measure for preventing data leaks. By ensuring that shared links have appropriate access controls in place, the organization can minimize the risk of unauthorized individuals gaining access to sensitive information. Restricting access to employees ensures that only authorized individuals with a legitimate need for the information can access it, reducing the likelihood of accidental or intentional data leaks.* |

| | |
|---|---|
| | *In addition, regular audits of access to team files by managers and security teams play a significant role in limiting the exposure of sensitive information. These audits enable the identification and prompt revocation of access privileges that are no longer required or have become excessive. By regularly reviewing and adjusting access permissions, the organization can maintain a least privilege environment, where employees have access only to the resources necessary for their job roles. This practice minimizes the potential for accidental data leaks caused by unauthorized access to sensitive information.*<br>*By implementing these measures, the organization strengthens its information privacy practices, reduces the risk of data leaks, and maintains a higher level of control over access to sensitive files. These actions align with industry best practices and provide a robust justification for improving data handling security within the company.* |

## Security plan snapshot

The NIST Cybersecurity Framework (CSF) provides a structured approach to organizing information related to security. It follows a hierarchical, tree-like structure, moving from broad security functions to specific categories, subcategories, 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 scenario, the implemented controls aimed at protecting against data leaks are defined in NIST SP 800-53. This publication serves as a comprehensive set of guidelines for securing the privacy of information systems. It outlines a wide range of security controls that organizations can implement to safeguard their data and mitigate the risk of data leaks.

It is common practice to hyperlink references in the security plan to the corresponding guidelines or regulations they relate to. These hyperlinks make it easy to access additional information about specific controls and gain a deeper understanding of how they should be implemented. It is typical to find multiple links to different sources in the references column, enabling individuals to explore various resources for detailed guidance on control implementation.

By utilizing the NIST SP 800-53 guidelines and establishing hyperlinks to relevant sources, the organization can effectively leverage industry-recognized best practices to develop a robust security plan and ensure the protection of sensitive data against leaks and unauthorized access.

Note: It is essential to keep the security plan updated with the latest references and guidelines as new versions or updates to NIST SP 800-53 or other relevant sources are released to stay aligned with evolving best practices and regulatory requirements.

## NIST SP 800-53: AC-6

NIST SP 800-53 is a framework developed by the National Institute of Standards and Technology (NIST) to assist businesses in creating a customizable information privacy plan. It serves as a comprehensive resource that outlines a wide range of control categories, including AC-6.

AC-6 specifically addresses the control requirements related to the principle of least privilege. Within NIST SP 800-53, each control provides essential information to guide organizations in implementing effective security measures:

- **Control:** This section presents a clear and concise definition of the security control, in this case, AC-6, which focuses on least privilege.

- **Discussion:** The discussion section within NIST SP 800-53 offers a detailed description of how the control should be implemented. It provides guidance on the specific steps, processes, and considerations involved in adhering to the principle of least privilege. This includes recommendations on access restriction, user role definitions, and proper authorization mechanisms.

- **Control Enhancements:** NIST SP 800-53 also offers control enhancements as supplementary suggestions to improve the effectiveness of the control. These enhancements provide additional measures that organizations can consider implementing to enhance their least privilege implementation. They might include practices such as regular access reviews, multifactor authentication, or automated tools for privilege management.

By referencing NIST SP 800-53: AC-6, businesses can access a wealth of information to aid in the implementation of least privilege controls. The control definition, discussion, and control enhancements provided within the framework offer a comprehensive guide for organizations to establish robust least privilege mechanisms, ensuring that access to sensitive resources is limited to only those with a legitimate need, thus reducing the risk of data leaks and unauthorized access incidents.

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