Project

In this project, I was tasked with enhancing data security by implementing measures to prevent data leaks. One of my key objectives is to configure shared links to internal files to ensure that access is limited exclusively to authorized employees, preventing unauthorized external access. Additionally, I will establish a systematic process for managers and security teams to conduct routine audits of access permissions for team files. This will help identify and address any inappropriate access rights, thereby reducing the risk of sensitive information exposure. Through these strategies, I aim to strengthen our data protection protocols and safeguard sensitive information from potential leaks.

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)	*The data leak occurred due to excessive access privileges and poor access management. The manager failed to revoke access to sensitive documents after sharing, while the customer success representative inadvertently shared an overly permissive link. Lack of oversight in information sharing and inadequate training on proper data handling procedures exacerbated the issue.*
Review	*NIST SP 800-53 AC-6 promotes data privacy by implementing least privilege principles, requiring minimal access for users and processes, and recommending enhancements like authorizing security function access, using non-privileged accounts for nonsecurity tasks, and auditing privileged actions.*

Recommendation(s)	*Access to sensitive resources should be restricted according to user roles. Additionally, it is important to conduct regular audits of user privileges to ensure that access rights remain appropriate.*
Justification	*To mitigate future data leaks, implement two crucial safeguards: 1) Configure shared links to internal files for employee-only access, preventing unauthorized external viewing. 2) Establish a routine where managers and security teams regularly audit access permissions to team files. These measures will significantly reduce the risk of sensitive information exposure and strengthen overall data protection protocols.*

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. 4
- **Control enhancements:** A list of suggestions to improve the effectiveness of the control.

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.