Data leak worksheet

Incident summary: During a sales call, a business partner was sent a link granting access to internal documents related to a new product launch, including customer analytics and marketing assets.

Further investigation revealed that a manager had previously shared the folder with a customer success representative and neglected to revoke access afterward. This oversight resulted in a security incident.

Control	Least privilege
Issue(s)	*The factors that lead to information leak is the failure to implement the least privilege principle.* *The organization also has failed to comply with existing standard rules for sharing information outside the organization.*
Review	*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.*
Recommendation(s)	*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.*
Justification	*Restrict access to sensitive resources based on user role.* *Regularly audit user privileges.*

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: 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.