Data leak report

Incident summary: During a meeting, a sales manager gave their team access to a folder of confidential documents. The folder held documents linked to a brand-new product that hasn't yet been made public. Customer analytics and marketing resources were also supplied. After the discussion, the manager did not withdraw team members' access to the internal folder but did issue a warning about not sharing promotional materials with others before getting permission.

One of the sales team members neglected to remember the manager's warning while on a video conference with a business partner. The salesperson intended to send the business partner a link to the promotional materials so that they may distribute them to their clients. Instead, the salesperson unintentionally distributed a link to the internal folder. Later, under the assumption that it was promotional content, the business partner shared the link on their company's social media profile.

Control	**Least privilege**
Issue(s)	*The sales staff and the manager weren't the only ones who had access to the internal folder. The authorization to distribute the promotional content on social media with the business partner should not have been granted.*
Review	*NIST SP 800-53: AC-6 discusses how a company might use the least privilege to secure the privacy of its data. To increase the effectiveness of least privilege, it also offers control improvements.*
Recommendation(s)	● *Restrict access to sensitive resources based on user role.* ● *Regularly audit user privileges.*
Justification	*If shared links to internal files are only accessible by employees, data leaks can be avoided. Additionally, mandating management and security teams to routinely audit team file access would assist prevent the release of critical data.*

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.