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 Manager forgot to revoke access to the folder which led to the representative accidental sharing of the folder to the customer.* *The manager also assumed the representatives on the sales call were going to wait for approval to share the material rather than revoke access.*
Review	*The NIST SP 800-53: AC-6 addresses the protection against data leaks by setting guidelines of securing the privacy of information systems, this is a customisable privacy plan that follows the principle of least privilege. Privacy data such as PII, PCI DSS, HIPAA are to be secured, documents and audited to ensure data security.*

Recommendation(s)	• Restrict access to sensitive resources based on user role - this will prevent unauthorized users from accidentally storing sensitive information. • Automatically revoke access to information after a period of time. - Th ensures no unauthorized user can misuse this data by only having limited time access. • Keep activity logs of provisioned user accounts. - This is to document who has / had access to sensitive data.
Justification	*These recommendations will prevent unauthorized internal employees from storing sensitive data, unintentionally and intentionally by restricting access to areas of the network containing sensitive resources.* *Automatically revoking access to information after a period of time will ensure no unauthorized user can mishandle data as it will only be used for a specific task.* *Keeping logs of activity to sensitive data will keep every user who has access accountable for the distribution and handling of the 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.