### Incident Report: Data Leak 2024-08-28 #1

### Est. Yerbatero Khel Vanesa & Hnos. SA - Km. 85 National Route 14 San Vicente

Incident Summary: A sales manager shared access to a folder of internal documents with his team during a meeting.

The folder contained files associated with a new product that has not been publicly announced. It also included customer analysis and promotional materials.

After the meeting, the manager did not revoke access to the internal folder, but warned the team that he would wait for approval before sharing the promotional materials with others.

During a video call with a business partner, a sales team member forgot his manager's warning.

The sales rep intended to share a link to the promotional materials so that the business partner could distribute them to their customers.

However, the sales rep accidentally shared a link to the internal folder. The business partner later posted the link on his company's social media page, assuming it was the promotional material.

| Control | Minimum privilege |
| --- | --- |
| Affairs | Access to the internal folder was not limited to the sales team and the manager.  The business partner should not have been given permission to share the promotional information on social media. |
| Review | NIST SP 800-53: AC-6 addresses how an organization can protect the privacy of its data by implementing least privilege.  It also suggests control improvements to enhance the effectiveness of least privilege. |
| Recommendations | Restrict access to sensitive resources based on user role.  Periodically audit user privileges. |
| Justification | Data leaks can be prevented if shared links to internal files are restricted to employees only.  Additionally, requiring managers and security teams to periodically audit access to team files would help limit the exposure of sensitive information. |

Security plan snapshot

The NIST Cybersecurity Framework (CSF) uses a hierarchical tree structure to organize information.

From left to right, it describes a broad security function and then gets more specific as it breaks down into a category, subcategory, and individual security controls.

| Function | Category | Subcategory | Reference(s) |
| --- | --- | --- | --- |
| Protect | PR.DS: Data Security | PR.DS-5: Data leak protections. | NIST SP 800-53: AC-6 |

In this example, the implemented controls that the manufacturer uses to protect against data leaks are defined in NIST SP 800-53, a set of guidelines for protecting the privacy of information systems.

Note: References are often hyperlinked to the guidelines or regulations they relate to. This makes it easier to learn more about how a particular control should be implemented.

It is common to find multiple links to different sources in the reference columns.

NIST SP 800-53: AC-6

NIST developed SP 800-53 to provide organizations with a customizable system and information privacy plan. It is a comprehensive resource that outlines a wide range of control categories.

Each control provides some key data:

\*Control: A definition of security control.

\*Discussion: A description of how the control should be implemented.

\*Control Improvements: A list of suggestions for improving control effectiveness.

| AC-6 | Minimum privilege |
| --- | --- |
| Control:  Users should only be provided with the minimum access and authorization necessary to complete a task or function. |
| Discussion:  Processes, user accounts, and roles should be applied as needed to achieve least privilege.  The intent is to prevent a user from operating with privilege levels higher than necessary to achieve business objectives. |
| Control improvements:  Restrict access to sensitive resources based on user role.  Automatically revoke access to information after a period of time.  Maintain activity logs for provisioned user accounts.  Periodically audit user privileges. |

Note: In the access controls category, SP 800-53 lists least privilege sixth, that is, AC-6.