### **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)** | *What factors contributed to the information leak?*  *The first issue was that the manager did not revoke the access to the internal folder, this should have been done right after the meeting. The employee forgot the warning from the manager and intended to share a link to one of the materials in the folder but accidentally shared the whole folder instead.* | | |
| **Review** | *What does NIST SP 800-53: AC-6 address?*  *It addresses a control that should be implemented for the given situation and identifies how this control should be implemented and why it would stop what had happened. This then shows how the security control can be further improved for more security and uphold security posture mitigating potential future issues.* | | |
| **Recommendation(s)** | *How might the principle of least privilege be improved at the company?*   * Restrict access to sensitive resources based on user role. * Automatically revoke access to information after a period of time. | | |
| **Justification** | *How might these improvements address the issues?*  *Restricting access to sensitive resources would have stopped the rest of the team from accessing these materials and sharing them as the team manager could have the privilege to share this document with the team however the rest of the team shouldn't be able to share the file so restrictions depending on the users role would have stopped this. Automatically revoking access to information after a time period would have stopped the incident as the manager wouldn't need to remember to do it manually as humans typically forget to do something and are considered a weakness, setting up some automation to revoke access to anyone after the meeting would have prevented the folder to be shared.* | | |

### **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.