Activity Exemplar: Determine appropriate data handling practices

Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity.

Completed Exemplar

To review the exemplar for this course item, click the link and select *Use Template*.

Link to exemplar: Data leak worksheet

OR

If you don’t have a Google account, you can download the exemplar directly from the following attachment.

Assessment of Exemplar

Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.

Note: *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that your activity reflects your analysis of appropriate data handling practices.*

Next, review the details of the completed data leak worksheet:

Issues

Many people neglected to keep the confidential information private. The manager should have done a better job keeping track of the internal folder by limiting access to the representative and themselves. The customer also could have done a better job of communicating their plans to share the marketing information before posting it to social media.

Review

NIST SP 800-53 is a resource that's designed to help organizations address data privacy risks. The document defines security controls, describes implementation strategies, and suggests individual control enhancements. AC-6 is a section about access controls that relate to the principle of least privilege.

Recommendation(s)

Based on the suggestion of NIST SP 800-53: AC-6, the data leak might have been avoided with the following controls:

- *Automatically revoke access to information after a period of time.*
- *Regularly audit user privileges.*

Justification

Automating security tasks whenever possible is a good way to reduce the chances of human error. In this case, creating a policy that sets expiration dates for access links might have avoided the leak. Requiring managers to regularly audit who can access their files is another way that information could be kept private.