IT Security Guidance for Storing and Sharing Protected Data Level 1 (PL-1) on Google Drive

During the COVID-19 emergency, SDSU CIO and IT Security Office is opening an emergency exception and allowing CSU Protected Level 1 (PL-1) data to be stored in Google Drive.

To keep PL-1 data as secure as possible, the IT Security office has developed the following guidelines:

1. Overall Document Privacy

Set the document as **Private**, and only share with selected people. (Private option highlighted below):

- **Public on the web** - Anyone on the Internet can find and access. No sign-in required.
- **Anyone with the link** - Anyone who has the link can access. No sign-in required.
- **SDSU University** - People at SDSU University can find and access.
- **People at SDSU with the link** - People at SDSU who have the link can access.
- **Private (only use this option)** - Only people explicitly granted permission can access. Sign-in required.

2. Check Names

When sharing a document or folder, make sure you have the right person. For example, there may be an undergraduate student who has the same name as one of your co-workers.

3. Share with a Group

Did you know that Google Groups can be used to assign permissions to documents, especially in large departments? This can save a lot of time and ensure consistency.

4. Name Clearly

Be mindful of what you name folders and documents. People you share with will see the name, so you should be descriptive and professional in your naming. It might be helpful to include the name of the project or your department so it is easy for others to find.

5. Use Share Team Drives, Not Documents

If it is likely that you will share documents in the future with the same group of people, it is best to create a Shared Team Drive and share it with specified users. All the documents you put in that folder will be automatically shared with the same group of people.
• **Why?** Sharing individual documents is more time consuming and can lead to errors and inconsistencies. When sharing a folder, it is easier to keep track of who has access and give a new person the ability to access many files at once. Also, using a folder allows everyone in your group to add to that folder, creating an easy-to-find archive of group materials.

• **Why not?** If you only need to share one document, you may not need a folder.

• **Shared Drive Settings.** Use the following to ensure the most secure settings for Shared Team Drives.
  
  - Only people inside San Diego State University can be given access to the files in this shared drive.
  - Only members of this shared drive can access files in this shared drive.
  - Prevent commenters and viewers from downloading, copying, and printing files in this shared drive.

6. Protect Your SDSUid Password

• Don't reveal it to anyone
• Don't re-use it for other accounts

7. Do Not Attach Files With PL-1 Data to Email Message

• Only use Google drive and Google team Drive to store files with PL-1 data. Do not attach and email files with PL-1 data.

8. Document Deletion

• Only the creator/owner can permanently delete a doc/collection. If something has been moved, the owner can still find it in the "Owned by Me" section of their Google Docs/Drive homepage. If the owner is no longer at SDSU, the item(s) may be deleted permanently. For document preservation, we recommend using Google “Team drive” instead of “My Drive”.

• When deleting a file, the file is sent to Google Trash. Only once permanently deleted from the trash, Google Docs and collections cannot be recovered.
9. Use Google’s "Account Activity" Feature to Help Make Sure No One Else is Using Your Account

Your Recent Activity – Entire Google Account

- The "Recent activity" section of your Account Security page lists security-related actions you’ve taken, such as signing in to your Google Account, changing your password, or adding a recovery email address or phone number. This information is for your entire Google Account, so sign-ins from any Google product (such as Blogger, Gmail, or YouTube) will be listed in this section.

- If you notice anything suspicious, e.g. a sign-in from a browser you've never used, or a location you've never been to, you are prompted to change your password to secure your account. If you notice a recovery option change you did not make, be sure to update the recovery option in addition to changing your password.

10. Sign Out of Your Google Account When You're Not Using It

11. Do Not Connect to Your G Drive on Public Computers