# Data Security in CTAC Google Drive:

Google Drive is a cloud-based technology managed by Google – one of the leading technology companies worldwide. Cloud-based solutions are automatically kept up-to-date and protected against vulnerabilities by Google security engineers, some the world's foremost experts, who work to ensure that data is not compromised. Google Drive itself has never fallen victim to a major cyber security incident.

Some popular competing cloud storage services include: Dropbox and OneDrive.

**Encryption.**

Google encrypts data within Google Drive. All files uploaded to Drive are encrypted in transit (i.e., while being editing, or active) and at rest with Advanced Encryption Standard (AES) 256-bit encryption. The AES is a symmetric encryption algorithm and one of the most secure. The United States Government uses it to protect classified information, and many software and hardware products use it as well.

**Access Controls.**

- CTAC controls who can access files in Google Drive.
- CTAC only provides access to users with a legitimate reason for accessing the files (i.e., the Contract Manager, Research Planning and Evaluation Coordinator, Program Staff, etc.)
- Each program only has access to their own data.
- Staff have been advised to only share the private link with authorized users.
- Authorized users must login with a username and password.
- Google passwords must be a minimum of 8 characters and a mix of letters, numbers, and symbols. It is also recommended not to reuse passwords from other accounts.

**Multi-Factor Authentication.**

- When logging in from a device other than the one typically used, Google will prompt the user for additional verification before providing access. This is called multifactor authentication (MFA) and will require the user to provide a passcode received via text or email to validate they are indeed an authorized user.

**Intrusion Protection.**

- Google monitors for any unusual, unauthorized, or suspicious activity. Additionally, the account owner, CTAC, receives notifications and monitors all account activity.