Purpose: The intent of the following policy is to define data security issues that specifically relate to Data Integrity and address the authorization, validation, modification controls, and consistency of data.

Policy: CDS will maintain system's integrity controls sufficient to meet all legal, ethical, and business requirements. These controls must protect data against improper alteration or destruction during processing and during storage.

Procedure and/or Process:

CDS is ethically and morally committed to its participants and stakeholders to establishing and maintaining an effective self-governance program that prevents, identifies, and rectifies any data integrity problems.

Authorization:
- All input to production computer systems, which has been submitted for processing is completed by properly authorized personnel.
- Data input must be linked to standard approved source documents completed by authorized personnel.

Validation:
- Systems have reasonable input and edit validation checks built into them.
- Transactions which fail such checks, must be returned to the submitter for correction and resubmission.
- Monthly validation checks are conducted to further ensure data integrity.

Modification Controls:
- Edit accessibility controls are built into CDS systems.
- Edit tracking for critical information is built into CDS systems.
- Edited information is subjected to the same validation procedures that original input transactions receive.

Consistency of Data:
- Standard forms are developed, updated, and maintained.
- Personnel receive ongoing training on the utilization and interpretation of all CDS forms.
- Saved documents must use modern file extensions. I.e.: .docx for Word files, .xlsx for Excel files, etc. This is to ensure long-term future compatibility. Old forms and other frequently used template files must be updated to new formats when applicable.