DATA SECURITY

Schedule and Supporting Documents

OVERVIEW

Background:

Data security is a paramount problem in the industry. In the wake of numerous recent data breaches, data security has become a strategic issue for life insurance providers. Tighter regulations combined with new CITS data feeds containing more and different types of data and new players in the market have put the need for CLIEDIS to provide direction on data security requirements.

As carriers reevaluate their security requirements and look to better validate compliance, distributors seek a consistent set of requirements to adhere to.

When carriers provide CITS data feeds, they require the data to be appropriately secured. Today, each carrier establishes its own set of data security requirements that the recipient (and its IT Service Providers processing the data) must abide by.

A carrier does not achieve competitive advantage by having different security requirements than someone else. The data sent to a distributor and their corresponding systems is being secured the same way, irrespective of who is sending the data.

Industry Landscape:

- Over 80 distributors in Canada receive CITS data feeds today.
- CLIEDIS has 14 carrier members who are either sending or considering sending data feeds.
- CLIEDIS has 16 solution provider members that deal directly with client and policy data for distributors and advisors, a fraction of the providers that touch the data.
- Each distributor utilizes multiple systems and IT solution providers for managing their business.

Each distributor along with their solution providers must understand and be compliant with the security provisions defined by each carrier they work with.

The agreements need to be unambiguous, consistent and reasonable to ensure that every player in the industry understands and can comply to the requirements.

CLIEDIS carrier members and representatives from CAILBA collaborated to address these concerns. Through this effort, CLIEDIS has developed a single set of data protections that can be applied to all confidential data received by trading partners across the industry, not only to CITS data feeds.

Purpose:

The purpose of the schedule and corresponding documents is to establish a clear and single set of requirements and conditions that distributors and their corresponding IT service providers, host providers, trading partners and advisors can comply with. These conditions will define what a Recipient can and must adhere to in order to receive electronic data feeds from the Sender and meet the Sender's security obligations. As an industry we want to:

- Ensure Data is **Secure**
- Ensure Security is **Achievable**
- Ensure Protections are **Consistent**
- Ensure Restrictions are **Realistic**

Documents Provided:

The following documents work in concert with one another to provide a complete package of information:

- CLIEDIS Data Security Schedule
    - This document defines a single set of data protections that serves as a schedule used alone or in conjunction with an existing contract in place between trading partners.
- CLIEDIS Data Security Questionnaire
    - This questionnaire is aligned with each section of the Data Security Schedule. Its purpose is that, upon request, a company can document the methodologies and rules in place for achieving the protections defined in the schedule.
- CLIEDIS Data Security Schedule FAQs
    - These FAQs are aligned with each section of the Data Security Schedule. Its purpose is to augment the schedule, providing additional details and guidance for supporting and understanding the protections defined in the schedule.