iGT UNC ANCILLARY DOCUMENT

PASSWORD PROTECTION PROTOCOLS

DD MM 2018~~01st June 2017~~
Version ~~3~~4.0

Change History

Version	Change	Date
1.0	First Issue	December 2010
2.0	iGT044	22nd February 2013
3.0	iGT074S	1st June 2017
4.0	IGTXXX	DD MM 2018

~~i~~IGT UNC Ancillary Document

Password Protection Protocols

1. Introduction

This document sets out the operating principles for the password protection of specified "Protected Information" in the ~~i~~IGT UNC under Section K clause 23 - relating only to the provision of invoice supporting data and Portfolio Extracts sent between the Pipeline User and Pipeline Operators.

2. Password Preparation

Passwords are to be chosen by the Pipeline User, and will be a minimum of eight characters long and will contain at least one upper case character, one number and one special character - for example: F2CRes&A

If a Pipeline User has failed to provide the Pipeline Operator with a password, individual passwords will be created by the Pipeline Operator for those defaulting Pipeline Users to enable the Pipeline Operators compliance. All passwords will be unique to each Pipeline User and must conform to the above password configuration. The Pipeline Operator will then communicate this password to the Registered User.

Passwords are to change 3 times a year to coincide with the planned Network Code release times each year, so new passwords will be provided for use from the 1st March, 1st July and 1st December. ~~,~~ The ~~i~~IGT UNC Representative is required to remind parties of the forthcoming changes by putting the topic on the Modification Panel Agenda the month preceding the issue of the new passwords. In the event that a Pipeline User needs the passwords changed outside of ~~with~~ this timeframe~~table~~, the Pipeline Operator will do this, but no more than monthly.

The Pipeline Users will provide the passwords to the Pipeline Operator at least one month in advance of their application, should the password not be provided in the requisite timeframe, the Pipeline Operator can delay the application of the password for one calendar month. If the Pipeline User fails to provide a replacement password the Pipeline Operator will continue to use the last valid password until a new password is provided in the requisite timeframe.

Software utilised for password protection should be that contained within the software, where applicable (Microsoft applications) or for zipped files the default requirement would be WinZip7 (NB this is a commonly available product which is free to download.), unless both the Pipeline Operator and the Pipeline User agree an alternative.

3. Application of Passwords to Data

The password will apply to all types of email attachments and CD or DVD containing the above detailed data

Commented [KR1]: Is this requirement too specific to come from the IGT UNC? Maybe make this more generic?

Commented [KR2]: This contradicts the information below on when the Pipeline Operator will create passwords

Commented [KR3]: This is giving the option to change the password on a monthly basis so I would recommend saying the Pipeline Operator will do this on an ad hoc basis.

Commented [KR4]: What if a password has never been provided? This contradicts the information in the second paragraph which states that the Pipeline Operator will create a password if one has not been provided by the Pipeline User. This needs to be made consistent. E.g.: the Pipeline Operator will create a password in line with paragraph 2.

Commented [KR5]: Although this might be free to download, some organisations won't be able to download it if it is not supported by IT

Commented [KR6]: Is information sent by CD or DVD anymore?
I would consider changing this to USB.

In the event that the data covers a period over-arching a password change being applied, the password applied will relate to the start period of the data contained in the attachment. For example:

The 'Issue Date' is used to select the respective password. For example 20150102 (YYYYMMDD) – The January password would apply.

Invoicing ~~s~~Supporting ~~d~~Data

Th 'Start Date' is used to select the respective password. For example 02/01/2015 (DDMMYYYY) – The January password would apply.

For historic data previously provided before the implementation of this protocol, each Pipeline User will provide a password, conforming to the standard defined above, which will be used by the Pipeline Operator for the re-provision of any historic data of any period, which may also exceed a calendar month.

Commented [KR7]: We recommend that the password is related to the month it was sent not relating to the month the data is for

Commented [KR8]: This is a defined term