iGT UNC Ancillary Document

Password Protection Protocols

XXXXXX 20XX
Version 2.0

Change History

Version	Change	Date
1.0	First Issue	December 2010
2.0	iGT044	XXXXX 20XX

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 iGT UNC under Section K clause 23 - relating only to the provision of invoice supporting data and Portfolio Extracts and Customer with Special Needs files 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 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 out with this timetable, 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.

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:

Portfolio data covering the period 1st February to 30th April – the February password will 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.