

### Entitlement Control

---

This policy applies to customers and vendors subscribing to real-time market data in instances where they have technical and/or administrative control over the distribution of the data.

All entitlement control systems should have the ability to perform the following:

1. Each user entitled to real-time data must be assigned their own unique ID/Password which is not shared. For audit purposes, vendors are expected to maintain a record of all users entitled to data and a list of their respective user ID/Password's and entitlements.
2. Prevent uncontrolled simultaneous access to data by the same user ID/Password from more than one terminal.
3. Generate entitlement reports (i.e. .csv or .txt; not an Excel file) detailing by location, those persons entitled, and not entitled, to real-time market data. The system and/or report output should track the day and time each individual was permissioned or depermissioned and include the date the report was run, and the following fields:
  - a. User ID
  - b. VAN
  - c. Legal company name
  - d. Installation address
  - e. Number of entitlements (quantity)
  - f. Activation date
  - g. De-activation date
  - h. Type of data (Network A/Network B)
4. Provide an audit trail identifying each entitlement transaction (additions, deletions, etc.) on a product level

For audit purposes, all entitlement systems should have the ability to generate and store entitlement reports for a period of **no less than three years** from the date access to the data was removed. The reports must be made available to NYSE upon request or as determined from time to time. ***In the event a customer or vendor is unable to provide accurate historical/audit information from the entitlement system, NYSE reserves the right to bill for all devices on the network.***

Please refer to the NYSE Vendor Guide for reporting guidelines