LINK® System Security Overview

LINK® System Security Overview

- LINK® enables customers to establish and maintain security information related to their company using on-line screens. This information includes:
  - Basic company information such as name, type and DUNS
  - Addresses, Contacts and Notifications
  - LINK System Agreements
  - Local Security Administrator(s)
  - Users
  - Agencies
  - Affiliations

LINK® System Security Overview

- For external users, two types of companies can be established.
  - All Business Purposes
    - Business entity where users perform typical business functions such as requesting contracts, nominating, establishing PDAs, reviewing allocations or obtaining invoices.
  - Upstream/Downstream
    - Business entity where it is used solely as an upstream or downstream entity for nomination purposes. No business functions are performed.

LINK® System Security Overview

- LINK® System Agreement
  - A LINK® System Agreement must be executed, or a valid service agreement must exist, before access is granted to Enbridge pipelines or Storage facilities.
  - The agreement binds the executing company to the terms and conditions of the appropriate tariff.
  - The agreement must be executed by someone authorized to bind the requesting company to such legal agreement.
  - Business Units covered by individual agreements include:
    - TETLP, AGT, ETNG, EHP, MBHP, SGSC, BGS, BSP, OGT
    - BIG
    - MNUS
    - Southeast Supply Header
    - Steckman Ridge
    - Manta Ray
    - MNCA
    - Ozark Gas Gathering
    - Garden Banks
    - Mississippi Canyon
    - Nautilus
    - NEXUS, NEXUS Canada
    - Sabal Trail
    - Valley Crossing

LINK® System Security Overview

- Local Security Administrator
  - Each pipeline or storage facility tariff requires a Local Security Administrator for an “All Business Purposes” company.
  - The Local Security Administrator is responsible for:
    - Establishing and maintaining Service Requester contact and notification information.
    - Creating and managing individualized user ids.
    - Creating and modifying appropriate security rights for each user id.
    - Maintaining user account information.
    - Adding and terminating user ids when a status change occurs.
    - Monitoring the use of the individual user ids.
    - Resetting passwords for users if the self service method is not utilized.
  - We recommend having a backup Local Security Administrator in case the primary is out of the office.

LINK® System Security Overview

- Contact Information
  - Pipeline and Storage tariffs require customers to maintain contact information.
  - Contact information includes
    - Names (person or department).
    - Addresses.
    - Notification associations.
    - E-mail addresses.
    - Telephone numbers.

LINK® System Security Overview

- Contact Information
  - Contact uses define how a contact is used.
    - For example, if Enbridge has a question about who to contact regarding nominations, the person assigned the "Nominations" contact use type would be called.
  - Customers can define key contacts to receive important e-mails.
    - For example, the person assigned the “Mail/Deliver Invoice To” contact use type would receive an e-mail notification when monthly invoices are ready.
  - Every service requester must have at least one default General Use contact. This person would receive correspondence for other contact use types (such as Nominations or Mail/Deliver To) if a contact for that particular use type is not specified.
  - More than one person can be configured for a contact use type. In that case, the person or department marked as the "default" contact use type would be contacted first.

LINK® System Security Overview

- Agency Relationships
  - LINK® Security provides the ability for one business entity to act as an agent for another business entity in order to manage or view business activities.
  - Agencies are established by Enbridge business units. If a principal has an agent for two (or more) business units, two (or more) agencies must be established.
  - The agency can be for all of a business entity's functions or only a subset of those functions. Within a specific function, agencies can be assigned more granularly to a contract or meter level. Functions that can be assigned for an agency include:
    - Capacity Release - Perform Capacity Release functions or view capacity release information. This can be contract specific.
    - Contracting – Request, maintain or view contract information. For existing contracts, this can be contract specific.
    - Nominations – Perform nominations or view nominations for all contracts, a group of contracts or a single contract.
    - Meter Confirmations – Confirm meters, set PDAs, view allocations and imbalances for all meters/contracts or a subset of those.

LINK® System Security Overview

- Agency Relationships
  - OBA Imbalance Verifier – update OBA verification information for all OBA contracts or a subset of contracts.
  - View Invoice – view invoice information.
  - View Measured Volumes – view measurement information for all meters, a group of meters or a specific meter.
  - Update for Order 698 Power Plants – update power plant information resulting from Order 698.
  - View Gas Quality – view gas quality information for all meters, a group of meters or a specific meter.

  – Either the Principal or Agent can submit a proposal to create or amend an agency relationship through on-line screens.

  – The Principal may select to retain their update rights as well as assign such rights to an agent.

  – A Principal may assign an Agent the right to see data prior to the Agency.

  – A Principal can allow the Agent to act as their Local Security Administrator.

LINK® System Security Overview

- Agency Relationships
  - A Principal can allow the Affiliates of Agent to access the Principal's data.
  - Per tariff, agency relationships must be renewed on an annual basis.
  - E-Mail warnings will be sent to the Local Security Administrator of the Principal and Agent 60 and 30 days before an Agency expires.
  - Upon an Agency expiration, an e-mail notification will be sent to the LSA of both the Principal and the Agent.

LINK® System Security Overview

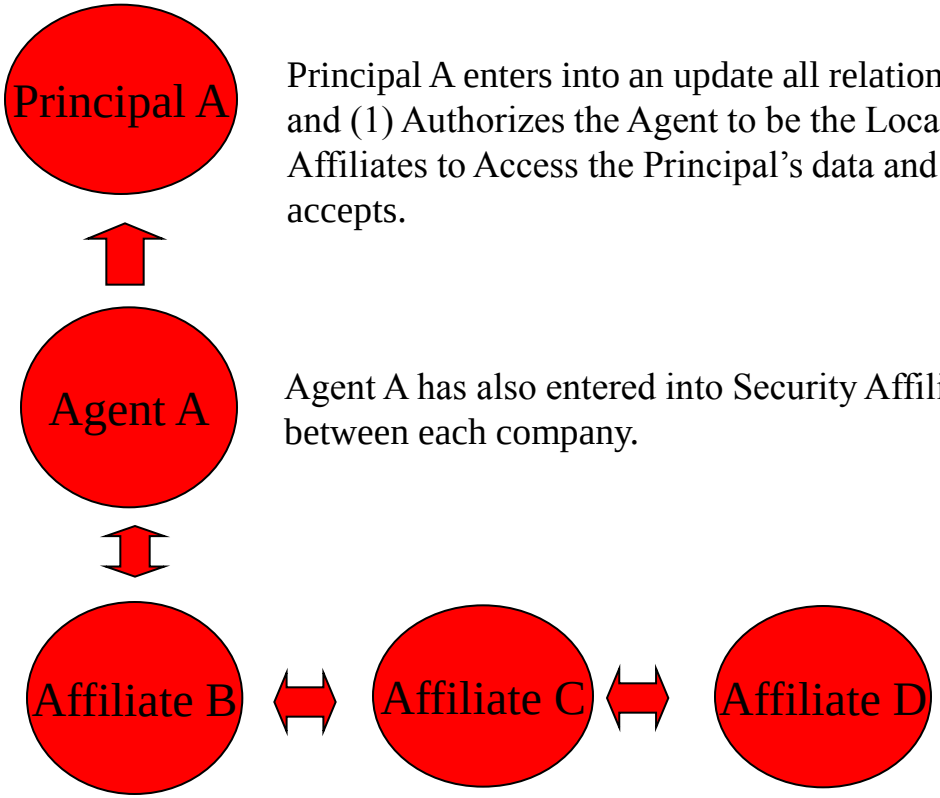
- Affiliations
  - LINK® provides the ability for access to be shared between a group of Affiliated companies. Not to be confused with Marketing Affiliations, Security Affiliations simply means a group of business entities that are closely related.
  - Affiliations can be proposed or amended by any party, but must be confirmed by the counter parties.
  - Local Security Administrator access can be shared if desired as an optional component of the Affiliation.
  - Affiliations are an all or nothing option since they are at a business entity level. However, the Security Administrator of one company in an Affiliation, can chose not to assign specific rights to employees from other business entities involved in the Affiliation.

LINK® System Security Overview

- While LINK® provides substantial security functionality and flexibility, customers should contemplate whether they have configured their security in an appropriate way. This is especially relevant with the pass through that can be allowed with Agencies or Affiliations.

- Lets examine the security setup on the next slide.

LINK® System Security Overview



Principal A enters into an update all relationship with Agent A. Agent A creates the proposal and (1) Authorizes the Agent to be the Local Security Administrator, (2) Allows the Agent's Affiliates to Access the Principal's data and (3) Allows the Agent to view prior data. Principal A accepts.

Agent A has also entered into Security Affiliation with Affiliates B, C and D and shared LSA's between each company.

However, Security Affiliate D is the competitor of Principal A. Because of the rights that have been established in the chain beginning with Principal A, Competitor D has full access to Principal A's data and can manage user ids of Principal A.