Joint Exchange
Information Barriers Policy

Document Version: 2.00 **Issue Date:** 2019.11.13

Public Documents for your use:

The LME Information Barrier Rules were published by the London Metal Exchange to outline rules for LME Warehouses, and prevent access to market-sensitive information ahead of public knowledge. These rules can be found at: https://www.metroftz.com/employees.html:

Background:

A. **MITSI Holdings LLC ["Metro"]** is an owner of LME Warehousing companies.
B. **Hyphen Resources LTD**., and, potentially, other companies to be created in the future [collectively, "**TradeCo**"] are companies that are permitted to enter into LME Contracts or buy and trade metal that is deliverable against an LME Contract. Both Metro and TradeCo are wholly-owned subsidiaries of **Reuben David Reuben and Simon David Reuben ("Reuben").**
C. On July 2nd, 2014, The London Metal Exchange [the "LME"] issued Notice 14/202 entitled **"INFORMATION BARRIERS BETWEEN WAREHOUSE COMPANIES AND TRADING COMPANIES", [the "LME Rules"],** which describes the requirements for Warehouse Companies to restrict the flow of information between the Warehouse and the Trading Company, when they are owned within the same Group.
D. It is essential from a regulatory, business principle and commercial perspective that Confidential Information relating to Metro and its business is not shared inappropriately, and therefore it is imperative that the following Policies and Procedures [collectively, the "Policy"] are complied with.
E. This structure is designed to help ensure that Confidential Information which Reuben receives as a result of its ownership of Metro is not shared with those individuals engaged in sales and trading activities on the LME, or in the sale and trading of related products. Strict adherence by all personnel to the rules and requirements applicable to the handling of Confidential Information and the operation of the Information Barrier as set out in this Policy is therefore critical. These procedures apply to employees of both Reuben and Metro at all times, both during and outside of office hours.
F. This Policy should be read in conjunction with the Rules of the LME, and Terms not defined in this Policy (including the term "Confidential Information") shall have the meaning given to them in the Notices of the LME.

Policies:

The following Metro policies, [along with their respective Procedures], are designated according to their corresponding Audit Requirements in Paragraph #50 of the LME Rules.

THE NEED TO KNOW PRINCIPLE AND CONFIDENTIALITY POLICY:

A. Metro will place this Policy in a location accessible to all Metro personnel designated as "Authorised Individuals", and communicate this Policy to them within each calendar year. (see paragraph 16)

1. The Policy as well as the LME Rules, is kept on the Metro Website, at www.metroftz.com/employees.
2. The Policy is accessible to all Authorised Recipients

3. Metro will train employees in the Policy prior to providing them access to Confidential Information, and again each calendar year, in accordance with the following items.

B. Access to Confidential Information is not given to any person other than an Authorised Recipient and is, in each case, limited solely to the specific Confidential Information that the Authorised Recipient strictly needs to know in order to carry out their day-to-day responsibilities for the Related Warehouse Company (see paragraph 18).

Overarching all of the procedures and requirements set out below is the "need to know' principle:

> **Confidential Information may only be shared with those individuals who could not carry out their responsibilities without access to such Confidential Information, and only to the extent required to enable them to carry out those responsibilities.**

Those Metro employees, directors, officers, agents, contractors or consultants designated to receive Confidential Information are defined as "Authorised Recipients".

You should not ask for or make an effort to obtain Confidential Information if you do not need to know the information. You are responsible for considering what information needs to be shared, in what form and with what level of detail before sharing any Confidential Information. Confidential Information should not be shared with others simply because this Policy allows it to be shared.

The determination of which documents are to be considered Confidential is to be carried out on a document-by-document basis. As an example:

- Employee A is permitted access to the Daily Stock Report, but not Financial Information.
- Employee B is permitted access to Financial Information, but not the Daily Stock Report.
- Therefore, Employee A is not permitted to forward the Daily Stock Report to Employee B.

C. Metro must continually assess what specific Confidential Information is necessary for each category of Authorised Recipient in order to carry out their day-to-day responsibilities and documents. (see paragraph 19);

1. The Definition of Confidential Information under the LME RULES:

Generally, common definitions of word “confidential” would include “secret, or private”. Generally, all information held by Metro should be kept strictly confidential, and be shared only by authorized personnel, and only with the owner of the material, or their designees.

The LME, in its Notice, created its own definition of the term “Confidential Information” [“Confidential Information”], which is more specific, and limited to information that could be defined as “commercially sensitive”, and could provide unfair advantage to a buyer and trader of metal, such as TradeCo. This definition reads as follows:

"Confidential Information" means, in respect of a Warehouse Company's business, any of the following, either ahead of general publication by the LME or while it remains commercially sensitive:

a. stock figures for LME deliverable metal;
b. all information relating to proposed or actual shipments of LME deliverable metal to be made or received by that Warehouse Company (including, in respect of shipments to be made by that Warehouse Company, any information of a commercially sensitive nature given to that Warehouse Company by the shipper, his agent or the recipient of that shipment, such as the identity of the customer, customs information, etc);
c. all information related to the issuance, holding and cancellation of LME warrants by that Warehouse Company; and
d. any other information in relation to specific LME brands which a Warehouse Company acquires through its warehousing activities.

2. What Metro does not consider Confidential Information:

a. **Warehouse Documents:** Metro has conducted a review of all of the documents that are generally available within the warehouse facilities, and has determined that they do not contain Confidential Information. These documents would include the following:
   i. **Individual Inbound and Outbound Bills of Lading:** Individual Inbound and Outbound Bills of Lading cannot be used for a commercial "inside" advantage, as they do not indicate warranting dates, and do not provide summarized information that would indicate large metal inflows or outflows. However, summarized reports describing information on the Bills of Lading could be considered LME Confidential. For that reason, summarized reports should be limited to the Metro Secure Office areas (as defined below).
   ii. **Individual Warrant Receiver Sheets**: These also do not contain warranting dates, and are usually produced in limited numbers, and therefore cannot be considered to be of a summarized nature, allowing for commercial advantage.
   iii. **Truck Logs**: These also do not contain warranting dates, and in limited numbers, cannot be considered to be of a summarized nature, allowing for commercial advantage.
   iv. **Warehouse Locator**: These also do not contain warranting dates, and in limited numbers, cannot be considered to be of a summarized nature, allowing for commercial advantage. They also contain information that is already published by the LME. This information also does not contain Customer information.
   v. **Ship Order Requests**: These also do not contain warranting dates, and in limited numbers, cannot be considered to be of a summarized nature, allowing for commercial advantage. They also contain information that is already published by the LME. This information also does not contain Customer information.

b. **Certain Office Documentation:**

While the offices hold much of what would be considered Confidential Information, not all information would be considered Confidential. Information such as that listed below would be examples of non-Confidential Information:

i. Company Financial Reports and other data, [unless it accompanies other LME Confidential Information];
ii. Real Estate Information;
iii. General IT Information not related to security;

iv. General Office Information such as Policies, Procedures, Standard Forms, etc.

c. Best Practices:

i. If the information is less than 3 days old, contains customer-specific information, or includes information ahead of LME publication, you should note that it could be interpreted as Confidential Information.

ii. Metro shall not store information identified as Confidential Information within the warehouse facilities, and shall limit such data to the Metro offices, and devices held by Metro employees identified as Authorised Recipients.

3. What Metro does consider Confidential Information:

a. Key Concepts: A key distinction that defines Confidential Information is that it must be commercially sensitive. Items containing commercially sensitive information should have one or more of these characteristics:

i. Timeliness: The information is known by Metro ahead of the Market.

ii. Magnitude: The information describes volumes that allow for a commercial advantage.

iii. Customer-Specific: The information includes the company names of specific owners of metal, or their designees.

b. Examples: The following are specific examples of standard Metro documents that should be considered Confidential Information:

i. Stock Reports, prior to the publication by the LME.
Examples:

- Any Stock Report, created at the end of the day for reporting to the LME, would be considered Confidential until the LME Publishes the following morning.
- Any report that shows projected warranting dates, ahead of LME publication. After that data has been published by the LME, the data is no longer considered Confidential Information.

ii. Shipping Reports: Any inbound shipping report that shows metal received within the last three [3] days, or any outbound shipping report that shows planned outbound shipments.

iii. Inventory Balances: Inventory levels broken down by location and metal type including details on inflows, outflows, on-warrant inventory, off-warrant inventory and cancelled warrants. Examples would include: Warehouse Capacity Reports, Metal in Warehouse Reports, etc..

iv. Customer-Specific Information: Reports regarding inbound or outbound commitments for specific customers, [with the exception of reports generated for the benefit of an owner of metal, and regarding the owner's own metal].

v. Deal Book: Any freight incentives, discounted rent agreements, rent share agreements or commitments of any kind that indicate future financial agreements or inbound or outbound flows of metal would be considered Confidential.

vi. Funding Requirements: If requests, or reports that show funding requirements can indicate future inbound activity, such requests or reports would be considered Confidential.

c. **Best Practices:** If the information is less than 3 days old, AND contains customer-specific information, or includes information ahead of LME publication, you should note that it could be interpreted as Confidential Information.

4. **Types of Information Held Within Metro Offices:**
   Metro holds Confidential Information in the following forms:
   a. **Digital File Data**: Data in the Metro Dropbox may contain Confidential Information.
   b. **Solomon**: Data in Microsoft Dynamics SL 2015 ["Solomon"], as well as the reports produced, could be considered Confidential.
   c. **Email**: (Microsoft Exchange Server 365): Email messages that contain current or planned, summarized, or otherwise commercially-sensitive information could be considered Confidential.
   d. **Physical Confidential Information:**
   Any physical information in printed form that comports with the definitions of LME Confidential Information are to be considered Confidential.
   e. **Conversations / Phone Calls:** Discussions containing current or planned, commercially-sensitive information is considered Confidential.

D. Metro will maintain a current listing of all Authorised Recipients and Designated Individuals, and the nature of the Confidential Information to which they have access (see paragraph 20).

Metro will organize Authorized Recipients into the following categories, and track membership of each:

1. **AR Groups:** AR's are grouped by the AR's employment arrangement with Metro, as follows:
   - **Metro:** Provided access to all types of LME Confidential Information, in accordance with the Need to Know Policy;
   - **Consultant:** Provided information related to the specific tasks they were hired to perform;
   - **Services:** Only provided physical access to the secured office environment, not electronic or other data;
   - **Designated Individuals:** Not AR's; TradeCo employees with supervisory functions for both TradeCo & Metro.

2. **Job Role:** AR's are also grouped by the role they play in the Company, and provided access to specific information as follows:
   - **Management:** Access to all LME Confidential Information permitted.
   - **Marketing:**
     Email: Access to all LME Confidential Information permitted;
     Dropbox: Access to marketing-related folders permitted;
     Solomon: Allowed to marketing-related screens & reports permitted
     Sage: No access permitted.
   - **Operations:**
     Email: Access to all LME Confidential Information permitted;
     Dropbox: Access to operations-related folders permitted;
     Solomon: Access to operations-related screens & reports permitted;
     Sage: No access permitted.

- **Accounting:**
  Email: Access to all LME Confidential Information permitted;
  Dropbox: Access to accounting-related folders permitted;
  Solomon: Access to accounting-related screens & reports permitted;
  Sage: Access to all information permitted.
- **Information Technology:** Access to all LME Confidential Information permitted.
- **Properties:** Access only to the secured office areas; viewing of hard copy LME Confidential Information is discouraged. No electronic rights permitted.
- **Consultant:** Access only permitted to LME Confidential Information in conjunction with their hired tasks;
  Dropbox: Access only to files shared by current AR's;
  Applications: Access only if required as a function of their tasks.
- **Developer:** A subset of Consultant; Developers can also change the programming of applications used to store LME Confidential Information. All other access rights the same as Consultant.
- **Janitorial:** Access only to the secured office areas; viewing of hard copy LME Confidential Information is discouraged. No electronic rights permitted.

3. **Location of Authorised Recipient Lists:** The lists of current members for each Security Group will be stored at www.metroftz.com/employees [Authorised Recipients tab] for viewing by the current Authorised Recipients.

4. **Designated Individuals**: There are a number of individuals within RB who have management or control responsibilities for both Metro and TradeCo [herein known as "Designated Individuals"]. These Designated Individuals are allowed to receive sensitive information (such as 401K, Tax, or other financial information), but are NOT allowed access to LME Confidential Information.
   - Confidential Information should NOT be shared with Designated Individuals, unless they are also an Authorised Recipient.
   - During meetings including Designated Individuals, Authorised Recipients shall be reminded of their responsibilities not to disclose Confidential Information during the proceedings.
   - In the event a Designated Individual is also an Authorised Recipient, Confidential Information should only be sent to these Authorised Individuals by Executives only (the"Funnel)":

5. **Need to Know for Consultants:** Since **Consultants** and **Developers** do not receive training on the full Policy (relying instead on the requirement not to send any information to anyone outside the Company), they will not be able to determine which Authorised Recipients have permission to receive specific access to LME Confidential Information. Therefore, personnel in these groups may only send LME Confidential Information to the Administrator (or the Administrator's Supervisors) of the system they are working on.

E. Designated Individuals will confirm on an annual basis that the information provided to them by Metro has complied with the requirements of paragraphs 17 to 20 of the LME Rules (see paragraph 20).

1. "Designated Individuals" are defined by the LME as:

   > "any individual who is a director or officer of both a Trading Company and a Related Warehouse Company who has management responsibility in relation to both such entities, or any individual who discharges a control function, including but not limited to compliance, legal, accounting, audit, treasury or tax in relation to both such entities."

2. For all Designated Individuals, Metro will require, once within each calendar year, a certification from all Designated Individuals stating that they have complied with these paragraphs. This Certification form can be found at our website at www.metroftz.com/employees [Training & Certifications tab].

PHYSICAL SEPARATION:

F) All Confidential Information (including any document containing or incorporating any Confidential Information), whether held in hard copy or electronic form, will be kept secure and properly protected against theft, damage, loss and unauthorised access (including by electronic means) (see paragraph 21);

1. **Physical Access:** Metro restricts physical access to electronic data sources, and physical paper documentation as follows:

AR Group / Job Role	Access Rights:
• Metro AR Group:	Unrestricted access to all secured offices.
• Services AR Group:	Unrestricted access only to the office in which they work.
• Consultants AR Group:	No access rights to any office. Must be treated like a visitor.
• IT Job Role:	Access to the Colocation Site & Servers.
• Designated Individuals:	No access rights to any office. Must be treated like a Visitor.

Visitors:

a. Only **Metro AR Group** members can provide access to Visitors.
b. Visitors, prior to entering the Metro Secure Office, will be required to sign into the sign-in log or iPad. Exceptions to this requirement are Governmental Agents [such as U.S. Customs Officers], and LME officials.
c. Visitors must be escorted while in the Metro Secure Office, to assure that the Visitor is not allowed to inspect LME Confidential Information on desks, or within files or computers in the office.

2. **Access to Servers:**

a. Servers at the colocation site, shall be restricted to those in the IT and Management Job Role groups only.
b. Servers within colocation facilities will be separately secured in rack cabinets with key access specific to Metro.
c. Metro will receive from their colocation service provider a Service Organization Control (SOC1) Report, covering the current calendar year.
d. In the event the SOC1 Report does not cover the entire calendar year, a Bridgewater letter will be provided to Metro to cover the period not covered in the SOC1 Report.
e. All servers are configured to include domain lockout of 30 minutes without activity.

3. **Paper Documents:**
   a. Authorised Individuals should not copy or remove any of the Confidential Materials from Metro's files for their own use,
   b. Document Destruction:
      - All Waste deemed LME Confidential will be shredded by the Company.
      - Authorised Individuals should use Metro-provided shred bins for any paper LME Confidential Information that is considered waste.

4. **Electronic Access:** Metro restricts electronic access to unauthorised parties in the following manner:
   a. Perimeter Security:
      i. **Fortigate 200D & 90D Threat Management Devices** are used to protect each Secure Metro Office with the following features:
         - Firewall,
         - Anti-Virus,
         - Intrusion Protection,
         - Application and Web Control [via FortiAnalyzer].

         Fortigate Administration is only open to IT Administrators.

      ii. **FortiAnalyzer is the repository of all network traffic inside Metro, including:**
         - identified virus's,
         - attempts to access blocked web sites (Malware, Phishing, or SPAM),
         - threats from outside / brute force attacks.
         - Reports are reviewed weekly to check for rogue elements operating inside the Metro network, and possible unauthorised access attempts.

      iii. **Open Ports** will be kept to a minimum, and where possible, restricted to access from and to specific ip addresses.

      iv. **SSID's:**
         - **Metro**: Used for laptops, printer, projectors and scanners that need access to the Metro Network. All phones and tablets are denied access to this.
         - **MetroIOS**: Used as a hidden SSID and only usable by Metro Issues phones or tablets that need Metro network access

- **MetroGuest**: Used for all other users, and guests that does not fall into one of the categories above. This is an isolated subnet that dumps directly to the internet. All devices are isolated from each other as well.

b. **Endpoints**:
   i. Computers are protected with Anti-virus and web protection via **FortiClient** program.
   ii. Servers: Anti-virus is installed on all servers, with the exception of the Exchange Server, which is protected by Microsoft Exchange's anti-spam/anti-virus features.
   iii. All machines are scanned for viruses in real-time [for individual files used], as well as on a weekly basis [for all files].
   iv. Individual Forticlient installations on endpoints upload all found violations to the FortiAnalyzer Server log, compiling an enterprise-wide event log.
   v. SmartPhones:
      - No mobile device is permitted to access the Metro network, unless the device is Metro-issued, and added to the approved MAC list in the Metro WiFi system.
      - Each device requesting email access is automatically placed in the Microsoft Exchange Server Device Quarantine. Devices will not receive messages (with the exception of webmail), until an Administrator approves the device to receive mail. Approval requires agreement to meet security requirements of requiring a passcode, and auto-locking within 5 minutes of no activity. Default acceptance is 1 minute.
      - If a device is lost, the user or supervisor must notify Administrator immediately. Administrators can send a remote wipe command to the device, which is left in place for at least 3 months. After that, the device can be removed from the server environment.

G) Access to Confidential Information by any individual who is not a relevant Authorised Recipient will be effectively restricted at all times (see paragraph 21);

Access to physical and electronic LME Confidential Information will be restricted as stipulated in other parts of this Policy.

H) All Confidential Information held within a computer system will be accessible only by Authorised Recipients using individual accounts and protected by a password or equivalent. Passwords will be changed at regular intervals and will meet best practice standards (see paragraph 22);

1. **Types of Passwords:**
   a. Microsoft Windows Active Directory passwords also control Solomon and Sage access via single-sign-on.
   b. No user accounts may be used by more than one individual.

2. **Microsoft Windows Logon Account:**

a. **Administration**: Windows logon accounts are administered by the Administrator account. Administrators are listed as Curt Felch and Scott Elwood.
b. **Control**: Windows Active Directory, on Windows Domain Servers, with the following settings:
   i. **Password Age**: Lockout after 90 days. New passwords cannot be the same as the previous password.
   ii. **Password Complexity:** Passwords must meet the following minimum requirements:
   - Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
   - Passwords must be at least six characters in length
   - Passwords must contain characters from three of the following four categories:
   - English uppercase characters (A through Z)
   - English lowercase characters (a through z)
   - Base 10 digits (0 through 9)
   - Non-alphabetic characters (for example, !, $, #, %)

   - **Exception**: The Administrator account will not have age limits, and will not be changed at any interval.

3. **SAGE Accounts:**
   a. **Administration**: SAGE Accounts are administered by **Brigid Callaghan**, ("SAGE Administrator").
   b. **Control**: User accounts are created by the SAGE Administrator. However, since SAGE has integrated Windows Authentication, logins are controlled by the Windows Logon Account per the rules of Section H.2 above, and there is no need for similar controls for Password Age or Complexity at the SAGE program level.

4. **Solomon Accounts:**
   a. Administration: Solomon Accounts are administered by Silvia Ramirez, ("Solomon Administrator").
   b. Control: User accounts are created by the Solomon Administrator. However, since Solomon has integrated Windows Authentication, logins are controlled by the Windows Logon Account per the rules of H.2 above, and there is no need for similar controls for Password Age or Complexity at the Solomon program level.

5. **Outside Consultants:**
   a. Accounts: Accounts for members of the **Consultant** and **Developer** AR Groups are limited to a specific duration, with a maximum of one (1) month.
   b. Passwords: Passwords for these Security Groups are set at 90 days, just like all other Windows passwords.

SEPARATION OF PERSONNEL:

I) All Authorised Recipients will be physically separated from the personnel of TradeCo. Where such personnel occupy the same premises, security

access systems will be installed to prevent unauthorised access (see paragraph 24);

1. TradeCo personnel [including those listed as Designated Individuals] will not be allowed to reside their primary place of business within Metro secured offices.
2. Authorised Recipients will be reminded not to allow TradeCo personnel to occupy offices adjacent to them, and monitor access to their desk from TradeCo personnel.
3. When TradeCo or RB personnel visit any Metro Secure Office, they will be treated as any other visitor, requiring them to sign in, and be escorted while in the office.

J) If a case arises wherein a Designated Individual is a director of both Metro and a TradeCo, Metro will have strict procedures in place regarding board meetings etc, to ensure that no Confidential Information is disclosed by that director to other personnel of TradeCo (see paragraph 25);

1. Metro does not generally conduct formal Board Meetings.
2. When Metro does conduct Board Meetings, or meetings that do include personnel in charge of TradeCo, the Senior Employee, or other designated employee, will sit in on Meeting to monitor information provided within the Board Meetings, and remind attendees of their obligations under the LME Rules.

AUTHORISED RECIPIENTS:

K) All Authorised Recipients will receive appropriate training upon commencing their role with Metro and periodically at least once in each calendar year thereafter (see paragraph 27);

1. **Forms of Training:** The training of the AR's differ based on the AR Group, as follows:
   a. **Metro:** Full PowerPoint presentation discussing each major concept of the LME Information Barrier Rules.
   b. **Consultant:** Abbreviated training reminding the prospective AR of their obligation under their NDA Agreement not to share any information with anyone outside of Metro.
   c. **Services:** Same as Consultants.

2. **Onboarding Procedures:** The following procedures should be followed for the onboarding of any new AR:
   a. **Request email:** A supervisor must send an email to Curt Felch requesting AR Status for the prospective AR;
      - Supervisor must state the desired AR Group and Job Role for the AR;
      - Supervisor must describe the access required [both physical and electronic];
   b. **Background Check:** Vetting practices must be completed in accordance with Section P below.
   c. **Training:** The prospective AR is required to take the Information Barriers Training in accordance with Section K.4 below;
   d. **Testing:** The prospective AR must complete a test in accordance with Section L below.

e. **Certification:** The prospective AR must provide a Certification in accordance with Section N below;
f. Instructions and forms for this onboarding procedure can be found at www.metroftz.com/employees [Training & Certification tab].

3. **Role Change Procedures:** Changes to access of existing AR's will require that the Supervisor make the request via email to Curt Felch.

4. **Recurring Training**: Existing Authorised Recipients will receive training, be required to pass a test, and sign an Information Barriers Certification at least once within each calendar year.

5. **Termination Procedures**: See Section Q below for specific procedures related to termination of ARs.

L) All Authorised Recipients must complete a Compliance Test upon the completion of their training, and at least once every two years thereafter (see paragraph 28);

1. **Forms of Testing:** Since the Policy for AR Groups differ, groups will have separate tests as follows.
   a. **Metro AR Group:**
      - Full test, with the following features:
        - 30 true/false questions
        - 100% correct scores are required.
        - Users can take the test as many times as they need to, in order to achieve the 100% score.
        - Wrong answers will result in the system providing additional information on that question.
        - Tests results are sent automatically to Curt Felch.

   b. **Consultant, Developer & Services AR Groups:**
      - Abbreviated test, meant to verify that the AR knows they must comply with the terms of their NDA, which is more restrictive than the LME Rules.
2. **RecurringTesting:** Testing for all AR's will be required prior to designation as an AR, and at least every two years thereafter.

M) Where any of the Authorised Recipients have failed to achieve a satisfactory result in a Compliance Test, Metro will take steps to provide appropriate additional training to such individual (see paragraph 28);

1. **See Policy L.1.a.**

N) All Authorised Recipients must sign a Compliance Acknowledgement (see paragraph 28);

Forms of Acknowledgement: Since the Policy for AR Groups differ, groups will have separate tests as follows.

1. **Metro AR Group:** Full Compliance Acknowledgement, stating they have been trained, tested, understand, and will comply with all of the LME Rules.

2. **Consultant, Developer & Services AR Groups:**
   - **Separate Confidentiality Agreement ("NDA"):** Members of these AR Groups are required to sign a **Confidentiality Agreement** ("NDA"). This agreement is far more restrictive than the LME Rules, in that it requires that the individual may not share any information with anyone outside of Metro, with the exception of other Authorised Recipients, and only for Metro-related business. This NDA is signed once prior to being designated as an AR.
   - **Abbreviated LME Certifications:** Members of these AR Groups must also sign an abbreviated acknowledgement, stating they understand that under the terms of their NDA Agreement, they cannot share any information with anyone outside of Metro. This Abbreviated LME Certification is to be signed prior to being designated as an AR, and thereafter, every two years.

O) Metro shall have internal sanctions for breach of this Confidentiality Policy, and such sanctions shall be strictly enforced (see paragraph 29);

Pursuant to the LME Rules, a breach of the procedures set out therein by either RB, TradeCo, or Metro may be regarded as an act of misconduct and may result in disciplinary action and the imposition of a severe financial penalty.

Metro takes any misuse, misappropriation, or improper dissemination of confidential information very seriously. Misuse and misappropriation of confidential information may violate contractual obligations, as well as the laws, rules and/or regulations of various jurisdictions in which Metro does business. It may also give rise to both civil liabilities and criminal penalties for Metro and for individual employees. In addition, even just the suggestion of misuse or misappropriation of confidential information can lead to serious reputational damage to Metro, TradeCo, and RB. Violations of this Policy and/or the Exchange Notice by employees may lead to disciplinary action, including dismissal, and any such violations may also need to be reported to regulatory or legal authorities and/or future employers. Metro reserves the right to take steps to vet any Authorised Recipient for their fitness and propriety to hold Confidential Information in accordance with **Policy P** below.

Internal sanctions for breach of this Policy will be considered on a case-by-case basis, and can include disciplinary action, demotion, dismissal, and additional legal action.

P) Metro shall have procedures to vet all Authorised Recipients to ensure that they are appropriate and suitable to handle Confidential Information (see paragraph 30);

Metro will vet all prospective AR's by completing a background check on each when possible.

In the event a background check is not possible [as may be the case with consultants, and foreign parties], some other form of vetting must be completed to indicate that the prospective AR is capable of keeping LME Confidential Information confidential.

Metro will also require a self-certification from each Authorised Recipient that since their date of hire, they have not been convicted of any local, state or federal crime, and has not been adjudged to be in violation of any local state or federal rules or regulations.

Q) Metro will take all reasonable steps to ensure that, as soon as possible upon becoming aware that any Authorised Recipient will cease to hold a role which requires access to Confidential Information and before the date on which the Authorised Recipient's role will cease, such Authorised Recipient has A) ceased to have access to any Confidential Information contained on any electronic device used by the Authorised Recipient; B) returned all documents and other materials (whether in hard copy or electronic form) containing or incorporating any Confidential Information to the Related Warehouse Company; and C) certified to the Related Warehouse Company in writing that (a) and (b) above have been complied with (see paragraph 31);

1. **Termination Procedures:** Metro's termination procedures are as follows:
   a. Supervisors, as soon as possible upon becoming aware that an Authorised Recipient will be terminated, or will no longer hold a role requiring access to Confidential Information, should fill out the Termination form at www.metroftz.com/employees [Hires, Changes & Terminations tab]. This will send an email to the appropriate parties to collect equipment issued to the employee, and make the appropriate changes to their status, to safeguard the company from monetary, document and equipment theft.
   b. The website will send an email to the appropriate parties requesting that they take the appropriate actions of removing account access, retrieving equipment, changing alarm codes, etc.
   c. Confirmation of these completed items should be sent via email to Curt Felch as a record of the termination of access.
   d. **Return / Destruction of Documents:** Supervisor, as soon as possible, will request that the terminated Authorised Recipient sign the Return of Documents Certification (also at the Metro employee website], and take all reasonable steps to make sure that any materials are returned, and the Certification is signed. The Supervisor shall make reasonable efforts to document their efforts to obtain any Confidential materials or the Certification, and forward them to Curt Felch.

R) Metro will keep and maintains up-to-date accurate written records [for a period of at least 6 years] the following items (see paragraph 32);

1. all training provided to Authorised Recipients;
2. the results of each Compliance Test;

3. all Compliance Acknowledgements;
4. any breaches of the Confidentiality Policy; and
5. any disciplinary sanctions imposed upon any Warehouse Personnel for any breach of the Confidentiality Policy.

Metro will keep copies of all records listed above for a period of at least 6 years.

SENIOR EMPLOYEE:

S) Policy: Metro will appoint a senior employee who is responsible for ensuring that the confidentiality procedures adopted to comply with this Notice are effective and are followed (see paragraph 33);

Procedures:

1. Metro's senior employee [as described in the LME Rules], [the "Senior Employee"] is responsible for the implementation and operation of confidentiality procedures at Metro.
2. The Senior Employee will be appointed by the Metro Board of Directors.
3. Currently, the Metro Senior Employee is **Curt Felch**.

TECHNOLOGY CONTROLS:

T) Metro's electronic systems are sufficiently robust to ensure that Confidential Information is protected from theft, damage, loss and unauthorised access (see paragraph 34);

See **Policy F** for security policies regarding electronic information.

U) Physical access to the production data centre(s) and systems storing Confidential Information shall be restricted to Authorised Recipients and other appropriate individuals with day-to-day responsibility for information technology and the data centre shall be protected from environmental hazards (see paragraph 34);

1. **See Policy F** for security policies regarding access to servers.
2. Visits to the Southfield, MI colocation site shall include observations when changes have been made to any building system that affect environmental conditions. In the event such changes have been observed, an email to Curt Felch should be sent to document the environmental system change.

V) Logical access to programs and data stores containing Confidential Information shall be restricted to Authorised Recipients with day-to-day responsibility for information technology (see paragraph 35);

See Policy H for administration of Microsoft Windows Active Directory, Solomon, and SAGE programs.

W) The change management process implemented shall ensure that changes to application and data stores containing Confidential Information, as well as changes to supporting system software, do not impact the logical access controls in place (see paragraph 36).

1. **Developer access** is limited to those in the **Developer** AR Group.
2. **Programs with Developer Access**: Solomon.
3. **Program Administrators**: See **Policy H** for the Authorised Recipients that are assigned as Administrators of each respective program.
4. Only the assigned Administrator for Solomon is authorized to make changes to Logical Access, and will monitor logical access rights for any changes, especially while Developers are completing their tasks.
5. **Periodic Review:** Logical Access rights shall be reviewed by Program Administrators on an annual basis.

DISCOUNTED LME WARRANTS:

1. TradeCo cannot sell or offer to sell LME warrants issued in respect of other Warehouse Companies operating in the same Location or within a 250 mile radius of the relevant Location at a discount to Metro's LME warrants, unless it can demonstrate that it would have offered the same discount even if Metro were not in the same Group.

2. TradeCo cannot offer any incentive to customers or exchange or substitute LME Warrants issued by Metro for LME warrants isueb y any other Warehouse Company's listed warehouse in the same Location or within a 250 mile radius of the relevant Location.

ACCESS TO WAREHOUSES:

1. No TradeCo personnel with responsibilities for Metro shall be permitted to inspect metal held on LME Warrant by TradeCo at another Warehouse Company.

DUTY TO INFORM THE LME OF BREACHES:

1. In the event that any Metro employee has reasonable grounds to suspect any breach of any breaches of the requirements of the LME Rules:
   a. That employee should notify their Supervisor of the suspected breach as soon as reasonably practicable,
   b. The Supervisor should notify the Senior Employee as soon as reasonably practicable,
   c. The Senior Employee should:
      i. Investigate the potential breach immediately, obtaining opinions from outside sources (auditors, legal counsel) if deemed necessary,
      ii. Report the findings to the Supervisor, Employee, and senior staff of Metro,
      iii. Keep a log of all potential and actual breaches,
   d. In the event the incident is deemed a breach of the Confidential Information Barrier Policy of the LME, the Senior Employee will:
      i. Notify the LME of the breach as soon as reasonably practicable, but not less than 24 hours after the breach is identified,
      ii. Determine any steps necessary to limit potential liability to Metro as a result of the breach.

2. In the event any employee feels that the breach was not reported properly, each employee has a general duty to inform the LME, in writing, of any breaches of the requirements of the LME Rules as soon as reasonably practicable.