# Schedule 1
# SECURITY and CONTINUITY OF THE CLEARING ACCESS SOLUTIONS

## 1 GENERALITIES

1.1 The Users accept notably but not exclusively the following obligations to maintain, throughout the term of this Access Agreement, the level of logical security and control of access to the Network Services, whatever the chosen Clearing Access Solution, governed by this Access Agreement;

1.2 The Users must promptly cooperate with LCH.CLEARNET in responding to security incidents and report to LCH.CLEARNET any event, condition, or activity that Users become aware of that indicates a possible or actual violation of the Users access rights, deviation or breach or compromise of the security of the Network Services.

1.3 The Users retain full control, either directly or indirectly, over the design and implementation of its policy of administering authorisations for logical access to the Clearing Access Solution on all of its sites (production site, back-up site).

1.4 Any change implemented at the Users' initiative must remain compliant with security standards.

1.5 The Users and LCH.CLEARNET will jointly investigate on all attempts at unauthorised access with a view to determining the causes and implement the most appropriate corrective solutions.

## 2 CONTINUITY AND SECURITY REGARDING NETWORK SERVICES

### *2.1 Continuity*

All network infrastructures shall comply with the following :

- resilient network equipment on Users' premises along with failover mechanisms
- resilient Users' access with no SPOF (Single Point Of Failure) based on dual carriers
- secured and fully-meshed network
- resilient central infrastructures

### *2.2 Security*

Security regarding encryption and authentication are guaranteed by the Network Services provided by LCH.CLEARNET, with end-to-end VPN (Very Private Network) tunnelling based on IPSec protocol (VPN gateway fully-managed by LCH.CLEARNET Network Services Subcontractors).

All clearing data sent through the Network Services are secured by this VPN layer:

- Real-time messaging MMTP
- File transfer FTP

In addition, each LCAP is isolated on a separate DMZ on LCH.CLEARNET central infrastructure.

# 3 CONTINUITY AND SECURITY REGARDING LCAP CLEARING ACCESS SOLUTION

## *3.1 Continuity*

In order to guarantee high availability and accurate performances of the LCAP, LCH.CLEARNET has implemented an architecture built on 3 levels of resiliency :

- Level 1 resiliency : Distributed Resource Scheduler (DRS) process;
- Level 2 resiliency : clusters architecture;
- Level 3 resiliency : Data Centres architecture with Disaster Recovery site;

## *3.2 Security*

The access to LCAP is handled through a Logical Dongle authentication.

# 4 SECURITY REGARDING ECCW CLEARING ACCESS SOLUTION

## *4.1 ECCW Member Security Administrator*

### 4.1.1 EMSA definition

The legal representative or any duly empowered representative of each User shall appoint at least one eCCW Member Security Administrator (EMSA) in charge of the management of the access to the eCCW Clearing Access Solution.

The EMSA shall have sufficient skills and independence to perform his/her tasks.

The EMSA shall be the sole point of contact for all security issues, and mainly:

- Definition/modification of member users profiles (reading / writing rights)
- Management of eCCW access cards.

The EMSA shall not use the eCCW Clearing Access Solution for any other purposes than those set out above.
LCH.CLEARNET strongly recommends the appointment of a supplemental EMSA in the event of any unavailability of the EMSA.

## *4.2 EMSA responsibilities*

### 4.2.1 User profiles management

LCH.CLEARNET will set up access to eCCW services in accordance with the terms set out on the eCCW Request Form and any instructions notified by the EMSA. LCH.CLEARNET shall make its reasonable endeavours to take into account this instruction within a reasonable delay upon receipt of the same and to the extent that such instruction is complete and compliant with the terms hereunder. This definition of profile(s) relies under the sole responsibility of the EMSA.

All following events shall be immediately communicated to LCH.CLEARNET by the EMSA in order to update Users' accesses:

- leavers (e.g. resignation, dismissal, any cause of leaving)
- change of function
- re assignation of eCCW access cards
- loss of token or activation of eCCW access cards following de-synchronisation or loss of PIN code.

4.2.2 Handling eCCW access cards

The EMSA shall distribute eCCW access cards to the duly appointed eCCW Users.

The EMSA shall further refer and comply with the appropriate Documentation.
The EMSAs shall train the eCCW Users in particular, with respect to the Security Policy detailed hereafter.

## *4.3 Security and continuity*

The following Security and Authentication Policy defines the eCCW security policies.

While signing the eCCW Request Form, the Users agree to comply with such Policy as detailed below and as amended from time to time.

4.3.1 Security and authentication policy

Authentication policy

The access to the eCCW Clearing Access Solution requires a unique username, a PIN code and a eCCW access card to generate the one-time password.

The user name identifies the eCCW services user and the PIN code enables the user to obtain a password from the eCCW access card. The eCCW access card generates a new password each time the user enters the PIN code.

To log into the eCCW services, the user shall enter his user name and password. The server authenticates the user and the eCCW system grants access to the user in accordance with the specifications set out in the Request Form.

A user name within the Users or any other entity identified in the Request Form enables the use of only one eCCW access card in a given environment (i.e. production and test platform for the main eCCW access card and production only for the eCCW backup access card).

User names will be provided by LCH.CLEARNET on request of the EMSA.
User names shall be meaningful enough to uniquely identify the user.
Very short names and generic names related to functions shall be prohibited.

The initial PIN is provided by LCH.CLEARNET for a fixed term. When an eCCW access card is used for the first time, the user will be requested to create a new PIN which can be changed at any time by the eCCW services user.
PINs shall be kept securely and shall not be disclosed. Any change of the PIN shall be undertaken under the responsibility of the relevant eCCW services user.

The eCCW Clearing Access Solution users shall securely store their eCCW access card when they do not use the same.

eCCW user sessions shall expire after a 20 minutes period of inactivity. The workstation which gives access to the eCCW services should also be configured with a separate, shorter local time-out option (e.g. Windows Screensaver).

In any case, the Users shall be responsible for the security and correct use of the eCCW access cards provided to them by LCH.CLEARNET. Any loss or misuse of eCCW access cards shall be the sole responsibility of the Users. In that respect, LCH.CLEARNET recommends EMSAs to order eCCW backup access cards to be assigned to eCCW users in back up situations.

Those eCCW backup access cards will be active and pre assigned to any eCCW user (i.e., duplication of the eCCW main access card), and as such to be used only in replacement of eCCW main access cards.

eCCW main access cards and eCCW backup access cards shall not be and cannot be used simultaneously.

# 5 SECURITY REGARDING LCH.CLEARNET WEB FIXED INCOME CLEARING ACCESS SOLUTIONS

The following Security and Authentication Policy defines the Web Fixed Income security policies.

While ordering a Web Fixed Income access Clearing Access Solutions, the Users agree to comply with such Policy as detailed below and as amended from time to time.

## *5.1 Authentication policy*

The access to LCH.CLEARNET relevant website (Web Fixed Income) is done through a secured link and requires a unique user ID, a PIN code and an access card to generate a one-time Pass Code.

The user ID identifies the user and the PIN code is used to activate the access card that will generate one-time Pass Codes on a regular basis. Those Pass Codes are synchronized with the relevant web site in order to be recognized.

To log into the Web Fixed Income services, the user shall enter his user ID and the one-time generated Pass Code that appears on his access card at login time. The server authenticates the user and the system grants access to the user.

## *5.2 Security and Back up Policy*

5.2.1 Member Security Administrator

### *5.2.1.1 MSA definition*

The legal representative or any duly empowered representative of each User shall appoint at least one Member Security Administrator (MSA) in charge of the management of the access to the Web Fixed Income Clearing Access Solution.

The MSA shall have sufficient skills and independence to perform his/her tasks.

The MSA shall be the sole point of contact for all security issues, and notably the management of Web Fixed Income access cards.

LCH.CLEARNET strongly recommends the appointment of a supplemental MSA in the event of any unavailability of the MSA.

### *5.2.1.2 MSA responsibilities*

#### *5.2.1.2.1 User management*

LCH.CLEARNET will set up access to Web Fixed Income services in accordance with the terms set out on the Web Fixed Income Request Form and any instructions notified by the MSA. LCH.CLEARNET shall make its reasonable endeavours to take into account this instruction within a reasonable delay upon receipt of the same and to the extent that such instruction is complete and compliant with the terms hereunder.

All following events shall be immediately communicated to LCH.CLEARNET by the MSA in order to update Users' accesses:

- leavers (e.g. resignation, dismissal, any cause of leaving)
- change of function
- re assignation of Web Fixed Income cards
- loss of token or activation of Web Fixed Income cards following de-synchronisation or loss of PIN code.

#### *5.2.1.2.2 Handling Web Fixed Income access cards*

The MSA shall distribute Web Fixed Income cards to the duly appointed Web Fixed Income Users.

The MSA shall further refer and comply with the appropriate Documentation.
The MSAs shall train the Web Fixed Income Users in particular, with respect to the Security Policy detailed hereafter.

5.2.2 Security

The Users are informed that this system creates an audit trail that cannot be repudiated. The users shall be held accountable for activities recorded identifying them as the perpetrators. Impersonation (Unauthorized use of one's identity and privileges) shall be avoided by protecting the secrecy user ID and access card.

The Users are responsible for taking the following precautions:

- PIN code shall not be spread over
- PIN code shall not be written on accessible documents
- access card shall be protected from the theft. If the access card is misled or stolen, LCH.CLEARNET CTH shall be informed at once to neutralize it so that it becomes unusable. LCH.CLEARNET CTH can generate a temporary password having made sure of the identity of the user.

The Users are responsible for the protection of their access cards:

- It shall not be immersed in a liquid
- It shall not be exposed to extreme temperatures
- It shall not be put under pressure
- It shall not be folded

# 6 SECURITY REGARDING CMS CLEARING ACCESS SOLUTIONS

## 6.1 Security and continuity

The following Security and Authentication Policy defines the CMS security policies.

While signing the Portal / CMS Request Form, the Clearing Members agree to comply with such Policy as detailed below and as amended from time to time.

6.1.1 Security and authentication policy

<u>Authentication policy</u>

The access to the CMS requires a unique username and a password.

To log into CMS, the user shall enter his user name and password. The server authenticates the user and the system grants access to the user in accordance with the specifications set out in the Request Form.

User names will be provided by LCH.CLEARNET on request of the user
User names shall be meaningful enough to uniquely identify the user.
Very short names and generic names related to functions shall be prohibited.

The initial password is provided by LCH.CLEARNET for a fixed term. When user logs in for the first time, the user will be requested to create a new password which can be changed at any time by the user.

### 6.1.2 Security and Back up Policy

CMS user sessions shall expire after a 20 minutes period of inactivity. The workstation which gives access to the CMS services shall also be configured with a separate, shorter local time-out option (e.g. Windows Screensaver).
The Clearing Member shall have in place all necessary security measures and procedures to prevent any unauthorised access to, or use of, CMS and CMS Content and the Clearing Member shall immediately notify LCH.CLEARNET in the event of any such unauthorised access or use, or if any Access Details are lost, stolen, misused or become known by any person other than the relevant Authorised User.

In any case, the Clearing Member shall be responsible for the security and correct use of the credentials provided to them by LCH Clearnet. Any misuse of the credentials shall be the sole responsibility of the Clearing Members.

The Clearing Member shall immediately notify LCH.CLEARNET on becoming aware of any unauthorised access or use, or if any of its Access Details are lost, stolen, misused or become known by any other person.

### 6.1.3 Continuity

The Clearing Member shall procure that the Authorised Users shall comply with the terms of this Access Agreement and shall ensure that only Authorised Users to whom valid Access Details have been issued will access or use (or attempt to access or use) CMS and that Access Details are at all times kept confidential. If an Authorised User ceases to be authorised to act by the Clearing Member, the Clearing Member will immediately notify LCH.CLEARNET by using the contact details provided for this purpose to the Clearing Member by LCH.CLEARNET from time to time. The Clearing Member shall ensure the Authorised User ceases to access and use CMS immediately if it ceases to be authorised to act by the Clearing Member.

LCH.CLEARNET shall be entitled to suspend access to CMS by the Clearing Member, suspend and/or terminate access to CMS in respect of each Authorised User, and amend any or all Access Details, in each case from time to time and without prior notice to the Clearing Member or any Authorised User. Where LCH.CLEARNET notifies the Clearing Member that it is suspending or terminating an Authorised User's right to access CMS the Clearing Member shall ensure that each Authorised User ceases to access CMS until, in the case of suspension, LCH.CLEARNET advises it that such Authorised User is no longer so suspended.

# 7 SECURITY REGARDING PORTFOLIO MARGIN CALCULATION TOOL

## 7.1 Security and continuity

The following Security and Authentication Policy defines the Portfolio Margin Calculation tool (PMC) security policies.

While signing the Portal / PMC Request Form, the Clearing Members agree to comply with such Policy as detailed below and as amended from time to time.

### 7.1.1 Security and authentication policy

Authentication policy
Clearing Members ID are assigned to individual users. They are created by nominated member Super Users or internal LCH business Super Users.

User authentication to the portal and its applications is two-factor.

1) A user ID and password will be required to login to the service
2) And a 2nd factor of authentication – based on source IP address (user's computer location) is invoked via a risk-based approach. i.e. users will be prompted for additional One-Time Access Code (sent to the registered corporate email address) when the source IP in non-white listed or is form a different location

Key Rules and Controls:

A named User ID and password are issued to each individual user. User IDs must not be shared and must only be used by the named individual. User IDs must be named and not generic and associated with a recognised corporate email account. 3rd party email addresses are not be allowed.
Passwords must conform to the following rules:

1) Minimum 8 characters.
2) At least one upper case.
3) One number
4) Passwords cannot be re-used (remembers 17 recently used passwords)
5) Passwords must be changed on first login or after reset by LCH Security Admin teams

The access to the PMC requires a unique username and a password.

To log into PMC, the user shall enter his user name and password. The server authenticates the user and the system grants access to the user in accordance with the specifications set out in the Request Form.

User names will be provided by LCH.CLEARNET on request of the Clearing Member. User names shall be meaningful enough to uniquely identify the user. Very short names and generic names related to functions shall be prohibited.

The initial password is provided by LCH.CLEARNET for a fixed term. When user logs in for the first time, the user will be requested to create a new password which can be changed at any time by the user.

### 7.1.2 Security and Back up Policy

PMC user sessions shall expire after a 30 minutes period of inactivity. The workstation which gives access to the PMC services shall also be configured with a separate, shorter local time-out option (e.g. Windows Screensaver).
Accounts that are not used for a period of 3 months will be made inactive and a further 3 months, deleted.
The Clearing Member shall have in place all necessary security measures and procedures to prevent any unauthorised access to, or use of, PMC and PMC Content and the Clearing Member shall

immediately notify LCH.CLEARNET in the event of any such unauthorised access or use, or if any Access Details are lost, stolen, misused or become known by any person other than the relevant Authorised User.

In any case, the Clearing Member shall be responsible for the security and correct use of the credentials provided to them by LCH.CLEARNET. Any misuse of the credentials shall be the sole responsibility of the Clearing Members.

The Clearing Member shall immediately notify LCH.CLEARNET on becoming aware of any unauthorised access or use, or if any of its Access Details are lost, stolen, misused or become known by any other person.

#### 7.1.3 Continuity

The Clearing Member shall procure that the Authorised Users shall comply with the terms of this Access Agreement and shall ensure that only Authorised Users to whom valid Access Details have been issued will access or use (or attempt to access or use) PMC and that Access Details are at all times kept confidential. If an Authorised User ceases to be authorised to act by the Clearing Member the Clearing Member will immediately notify LCH.CLEARNET by using the contact details provided for this purpose to the Clearing Member by LCH.CLEARNET from time to time. The Clearing Member shall ensure the Authorised User ceases to access and use PMC immediately it ceases to be authorised to act by the Clearing Member.

LCH.CLEARNET shall be entitled to suspend access to PMC by the Clearing Member, suspend and/or terminate access to PMC in respect of each Authorised User, and amend any or all Access Details, in each case from time to time and without prior notice to the Clearing Member or any Authorised User. Where LCH.CLEARNET notifies the Clearing Member that it is suspending or terminating an Authorised User's right to access PMC the Clearing Member shall ensure that each Authorised User ceases to access PMC until, in the case of suspension, LCH.CLEARNET advises it that such Authorised User is no longer so suspended.

#### 7.1.4 Auditing

All account activity with the portal and its applications is logged. Logs include: user name, source IP address, date, time, URL clicks and application action.
All changes to an individual access levels is tracked for audit purposes

# 8 SECURITY REGARDING CDSCLEAR REPORTING APPLICATION

## 8.1 Security and continuity

The following Security and Authentication Policy defines the CDSClear Reporting application security policies.

While signing the Portal / CDSClear Reporting application Request Form, the Clearing Members agree to comply with such Policy as detailed below and as amended from time to time.

### 8.1.1 Security and authentication policy

Authentication policy

User IDs are assigned to individual users. They are created by nominated member Super Users or internal LCH business Super Users.

User authentication to the portal and its applications is two-factor.

1) A user ID and password will be required to login to the service
2) And a 2nd factor of authentication – based on source IP address (user's computer location) is invoked via a risk-based approach. i.e. users will be prompted for additional One-Time Access Code (sent to the registered corporate email address) when the source IP in non-white listed or is form a different location

Key Rules and Controls:

A named User ID and password are issued to each individual user. User IDs must not be shared and only used by the named individual. User IDs must be named and not generic and associated with a recognised corporate email account. 3rd party email addresses are not be allowed.
Passwords must conform to the following rules:

1) Minimum 8 characters.
2) At least one upper case.
3) One number
4) Passwords cannot be re-used (remembers 17 recently used passwords)
5) Passwords must be changed on first login or after reset by LCH Security Admin teams

The access to the CDSClear Reporting application requires a unique username and a password.

To log into the CDSClear Reporting application, the user shall enter his user name and password. The server authenticates the user and the system grants access to the user in accordance with the specifications set out in the Request Form.

User names will be provided by LCH.CLEARNET on request of the Clearing Member. User names shall be meaningful enough to uniquely identify the user. Very short names and generic names related to functions shall be prohibited.

The initial password is provided by LCH.CLEARNET for a fixed term. When user logs in for the first time, the user will be requested to create a new password which can be changed at any time by the user.

### 8.1.2 Security and Back up Policy

The CDSClear Reporting application user sessions shall expire after a 30 minutes period of inactivity. The workstation which gives access to the CDSClear Reporting application services shall also be configured with a separate, shorter local time-out option (e.g. Windows Screensaver).
Accounts that are not used for a period of 3 months will be made inactive and a further 3 months, deleted.

The Clearing Member shall have in place all necessary security measures and procedures to prevent any unauthorised access to, or use of, the CDSClear Reporting application and the CDSClear Reporting application Content and the Clearing Member shall immediately notify LCH.CLEARNET in the event of any such unauthorised access or use, or if any Access Details are lost, stolen, misused or become known by any person other than the relevant Authorised User.

In any case, the Clearing Member shall be responsible for the security and correct use of the credentials provided to them by LCH.CLEARNET. Any misuse of the credentials shall be the sole responsibility of the Clearing Members.

The Clearing Member shall immediately notify LCH.CLEARNET on becoming aware of any unauthorised access or use, or if any of its Access Details are lost, stolen, misused or become known by any other person.

8.1.3 Continuity

The Clearing Member shall procure that the Authorised Users shall comply with the terms of this Access Agreement and shall ensure that only Authorised Users to whom valid Access Details have been issued will access or use (or attempt to access or use) the CDSClear Reporting application and that Access Details are at all times kept confidential. If an Authorised User ceases to be authorised to act by the Clearing Member the Clearing Member will immediately notify LCH.CLEARNET by using the contact details provided for this purpose to the Clearing Member by LCH.CLEARNET from time to time. The Clearing Member shall ensure the Authorised User ceases to access and use the CDSClear Reporting application immediately it ceases to be authorised to act by the Clearing Member.

LCH.CLEARNET shall be entitled to suspend access to the CDSClear Reporting application by the Clearing Member, suspend and/or terminate access to the CDSClear Reporting application in respect of each Authorised User, and amend any or all Access Details, in each case from time to time and without prior notice to the Clearing Member or any Authorised User. Where LCH.CLEARNET notifies the Clearing Member that it is suspending or terminating an Authorised User's right to access the CDSClear Reporting application the Clearing Member shall ensure that each Authorised User ceases to access the CDSClear Reporting application until, in the case of suspension, LCH.CLEARNET advises it that such Authorised User is no longer so suspended.

8.1.4 Auditing

All account activity with the portal and its applications is logged. Logs include: user name, source IP address, date, time, URL clicks and application action.
All changes to an individual access levels is tracked for audit purposes

# 9 SECURITY REGARDING CDSCLEAR TRADE MANAGEMENT APPLICATION

## 9.1 Security and continuity

The following Security and Authentication Policy defines the CDSClear Trade Management application security policies.

While signing the Portal / the CDSClear Trade Management application Request Form, the Clearing Members agree to comply with such Policy as detailed below and as amended from time to time.

### 9.1.1 Security and authentication policy

Authentication policy

Users ID are assigned to individual users. They are created by nominated member Super Users or internal LCH business Super Users.

User authentication to the portal and its applications is two-factor.

1) A user ID and password will be required to login to the service
2) And a 2nd factor of authentication – based on source IP address (user's computer location) is invoked via a risk-based approach. i.e. users will be prompted for additional One-Time Access Code (sent to the registered corporate email address) when the source IP in non-white listed or is form a different location

Key Rules and Controls:

A named User ID and password are issued to each individual user. User Ids must not be shared and only used by the named individual. User IDs must be named and not generic and associated with a recognised corporate email account. 3rd party email addresses are not be allowed.
Passwords must conform to the following rules:

1) Minimum 8 characters.
2) At least one upper case.
3) One number
4) Passwords cannot be re-used (remembers 17 recently used passwords)
5) Passwords must be changed on first login or after reset by LCH Security Admin teams

The access to the CDSClear Trade Management application requires a unique username and a password.

To log into the CDSClear Trade Management application, the user shall enter his user name and password. The server authenticates the user and the system grants access to the user in accordance with the specifications set out in the Request Form.

User names will be provided by LCH.CLEARNET on request of the Clearing Member. User names shall be meaningful enough to uniquely identify the user. Very short names and generic names related to functions shall be prohibited.

The initial password is provided by LCH.CLEARNET for a fixed term. When user logs in for the first time, the user will be requested to create a new password which can be changed at any time by the user.

### 9.1.2 Security and Back up Policy

the CDSClear Trade Management application user sessions shall expire after a 30 minutes period of inactivity. The workstation which gives access to the CDSClear Reporting application services shall also be configured with a separate, shorter local time-out option (e.g. Windows Screensaver).
Accounts that are not used for a period of 3 months will be made inactive and a further 3 months, deleted.

The Clearing Member shall have in place all necessary security measures and procedures to prevent any unauthorised access to, or use of, the CDSClear Trade Management application and the CDSClear Trade Management application Content and the Clearing Member shall immediately notify LCH.CLEARNET in the event of any such unauthorised access or use, or if any Access Details are lost, stolen, misused or become known by any person other than the relevant Authorised User.

In any case, the Clearing Member shall be responsible for the security and correct use of the credentials provided to them by LCH.CLEARNET. Any misuse of the credentials shall be the sole responsibility of the Clearing Members.

The Clearing Member shall immediately notify LCH.CLEARNET on becoming aware of any unauthorised access or use, or if any of its Access Details are lost, stolen, misused or become known by any other person.

9.1.3 Continuity

The Clearing Member shall procure that the Authorised Users shall comply with the terms of this Access Agreement and shall ensure that only Authorised Users to whom valid Access Details have been issued will access or use (or attempt to access or use) the CDSClear Trade Management application and that Access Details are at all times kept confidential. If an Authorised User ceases to be authorised to act by the Clearing Member the Clearing Member will immediately notify LCH.CLEARNET by using the contact details provided for this purpose to the Clearing Member by LCH.CLEARNET from time to time. The Clearing Member shall ensure the Authorised User ceases to access and use the CDSClear Trade Management application immediately it ceases to be authorised to act by the Clearing Member.

LCH.CLEARNET shall be entitled to suspend access to the CDSClear Trade Management application by the Clearing Member, suspend and/or terminate access to the CDSClear Trade Management application in respect of each Authorised User, and amend any or all Access Details, in each case from time to time and without prior notice to the Clearing Member or any Authorised User. Where LCH.CLEARNET notifies the Clearing Member that it is suspending or terminating an Authorised User's right to access the CDSClear Trade Management application the Clearing Member shall ensure that each Authorised User ceases to access the CDSClear Trade Management application until, in the case of suspension, LCH.CLEARNET advises it that such Authorised User is no longer so suspended.

9.1.4 Auditing

All account activity with the portal and its applications is logged. Logs include: user name, source IP address, date, time, URL clicks and application action.
All changes to an individual access levels is tracked for audit purposes

# 10 SECURITY REGARDING CDSCLEAR BACKLOADING APPLICATION

## 10.1 Security and continuity

The following Security and Authentication Policy defines the Backloading application security policies.

While signing the Portal / the Backloading application Request Form, the Clearing Members agree to comply with such Policy as detailed below and as amended from time to time.

### 10.1.1 Security and authentication policy

Authentication policy

Users ID are assigned to individual users. They are created by nominated member Super Users or internal LCH business Super Users.

User authentication to the portal and its applications is two-factor.

1) A user ID and password will be required to login to the service
2) And a 2nd factor of authentication – based on source IP address (user's computer location) is invoked via a risk-based approach. i.e. users will be prompted for additional One-Time Access Code (sent to the registered corporate email address) when the source IP in non-white listed or is form a different location

Key Rules and Controls:

A named User ID and password are issued to each individual user. User IDs must not be shared and only used by the named individual. User IDs must be named and not generic and associated with a recognised corporate email account. 3rd party email addresses are not be allowed.
Passwords must conform to the following rules:

1) Minimum 8 characters.
2) At least one upper case.
3) One number
4) Passwords cannot be re-used (remembers 17 recently used passwords)
5) Passwords must be changed on first login or after reset by LCH Security Admin teams

The access to the Backloading application requires a unique username and a password.

To log into the Backloading application, the user shall enter his user name and password. The server authenticates the user and the system grants access to the user in accordance with the specifications set out in the Request Form.

User names will be provided by LCH.CLEARNET on request of the Clearing Member. User names shall be meaningful enough to uniquely identify the user. Very short names and generic names related to functions shall be prohibited.

The initial password is provided by LCH.CLEARNET for a fixed term. When user logs in for the first time, the user will be requested to create a new password which can be changed at any time by the user.

### 10.1.2 Security and Back up Policy

The Backloading application user sessions shall expire after a 30 minutes period of inactivity. The workstation which gives access to the CDSClear Reporting application services shall also be configured with a separate, shorter local time-out option (e.g. Windows Screensaver).
Accounts that are not used for a period of 3 months will be made inactive and a further 3 months, deleted.
The Clearing Member shall have in place all necessary security measures and procedures to prevent any unauthorised access to, or use of, the Backloading application and the Backloading application

Content and the Clearing Member shall immediately notify LCH.CLEARNET in the event of any such unauthorised access or use, or if any Access Details are lost, stolen, misused or become known by any person other than the relevant Authorised User.

In any case, the Clearing Member shall be responsible for the security and correct use of the credentials provided to them by LCH.CLEARNET. Any misuse of the credentials shall be the sole responsibility of the Clearing Members.

The Clearing Member shall immediately notify LCH.CLEARNET on becoming aware of any unauthorised access or use, or if any of its Access Details are lost, stolen, misused or become known by any other person.

10.1.3 Continuity

The Clearing Member shall procure that the Authorised Users shall comply with the terms of this Access Agreement and shall ensure that only Authorised Users to whom valid Access Details have been issued will access or use (or attempt to access or use) the Backloading application and that Access Details are at all times kept confidential. If an Authorised User ceases to be authorised to act by the Clearing Member the Clearing Member will immediately notify LCH.CLEARNET by using the contact details provided for this purpose to the Clearing Member by LCH.CLEARNET from time to time. The Clearing Member shall ensure the Authorised User ceases to access and use the Backloading application immediately it ceases to be authorised to act by the Clearing Member.

LCH.CLEARNET shall be entitled to suspend access to the Backloading application by the Clearing Member, suspend and/or terminate access to the Backloading application in respect of each Authorised User, and amend any or all Access Details, in each case from time to time and without prior notice to the Clearing Member or any Authorised User. Where LCH.CLEARNET notifies the Clearing Member that it is suspending or terminating an Authorised User's right to access the Backloading application the Clearing Member shall ensure that each Authorised User ceases to access the Backloading application until, in the case of suspension, LCH.CLEARNET advises it that such Authorised User is no longer so suspended.

10.1.4 Auditing

All account activity with the portal and its applications is logged. Logs include: user name, source IP address, date, time, URL clicks and application action.
All changes to an individual access levels is tracked for audit purposes

# 11 SECURITY REGARDING CDSCLEAR COMPRESSION APPLICATION

## 11.1 Security and continuity

The following Security and Authentication Policy defines the Compression application security policies.

While signing the Portal / the Compression application Request Form, the Users agree to comply with such Policy as detailed below and as amended from time to time.

### 11.1.1 Security and authentication policy

Authentication policy

Users ID are assigned to individual users. They are created by nominated member Super Users or internal LCH business Super Users.

User authentication to the portal and its applications is two-factor.

1) A user ID and password will be required to login to the service
2) And a 2nd factor of authentication – based on source IP address (user's computer location) is invoked via a risk-based approach. i.e. users will be prompted for additional One-Time Access Code (sent to the registered corporate email address) when the source IP in non-white listed or is form a different location

Key Rules and Controls:

A named User ID and password are issued to each individual user. User Ids must not be shared and only used by the named individual. User IDs must be named and not generic and associated with a recognised corporate email account. 3rd party email addresses are not be allowed.
Passwords must conform to the following rules:

1) Minimum 8 characters.
2) At least one upper case.
3) One number
4) Passwords cannot be re-used (remembers 17 recently used passwords)
5) Passwords must be changed on first login or after reset by LCH Security Admin teams

The access to the Compression application requires a unique username and a password.

To log into the Compression application, the user shall enter his user name and password. The server authenticates the user and the system grants access to the user in accordance with the specifications set out in the Request Form.

User names will be provided by LCH.CLEARNET on request of the User. User names shall be meaningful enough to uniquely identify the user. Very short names and generic names related to functions shall be prohibited.

The initial password is provided by LCH.CLEARNET for a fixed term. When user logs in for the first time, the user will be requested to create a new password which can be changed at any time by the user.

### 11.1.2 Security and Back up Policy

The Compression application user sessions shall expire after a 30 minutes period of inactivity. The workstation which gives access to the CDSClear Reporting application services shall also be configured with a separate, shorter local time-out option (e.g. Windows Screensaver).
Accounts that are not used for a period of 3 months will be made inactive and a further 3 months, deleted.
The Clearing Member shall have in place all necessary security measures and procedures to prevent any unauthorised access to, or use of, the Backloading application and the Backloading application

Content and the Clearing Member shall immediately notify LCH.CLEARNET in the event of any such unauthorised access or use, or if any Access Details are lost, stolen, misused or become known by any person other than the relevant Authorised User.

In any case, the Clearing Member shall be responsible for the security and correct use of the credentials provided to them by LCH.CLEARNET. Any misuse of the credentials shall be the sole responsibility of the Users.

The Clearing Member shall immediately notify LCH.CLEARNET on becoming aware of any unauthorised access or use, or if any of its Access Details are lost, stolen, misused or become known by any other person.

11.1.3 Continuity

The Clearing Member shall procure that the Authorised Users shall comply with the terms of this Access Agreement and shall ensure that only Authorised Users to whom valid Access Details have been issued will access or use (or attempt to access or use) the Backloading application and that Access Details are at all times kept confidential. If an Authorised User ceases to be authorised to act by the Clearing Member the Clearing Member will immediately notify LCH.CLEARNET by using the contact details provided for this purpose to the Clearing Member by LCH.CLEARNET from time to time. The Clearing Member shall ensure the Authorised User ceases to access and use the Backloading application immediately it ceases to be authorised to act by the Clearing Member.

LCH.CLEARNET shall be entitled to suspend access to the Compression application by the Clearing Member, suspend and/or terminate access to the Compression application in respect of each Authorised User, and amend any or all Access Details, in each case from time to time and without prior notice to the Clearing Member or any Authorised User. Where LCH.CLEARNET notifies the Clearing Member that it is suspending or terminating an Authorised User's right to access the Backloading application the Clearing Member shall ensure that each Authorised User ceases to access the Backloading application until, in the case of suspension, LCH.CLEARNET advises it that such Authorised User is no longer so suspended.

11.1.4 Auditing

All account activity with the portal and its applications is logged. Logs include: user name, source IP address, date, time, URL clicks and application action.
All changes to an individual access levels is tracked for audit purposes