
Section 3

CCASS Terminals/CCASS Phone System/CCASS Internet System/ Participant Gateways

3.1 DIRECT LINKAGE

3.1.1 Use of PCs for direct linkage to CCASS

With the exception of Investor Participants and unless otherwise authorised by HKSCC pursuant to Rule 704, each Participant or its Settlement Agent is required to be directly linked to CCASS via dedicated data communication links through the use of a PC or multiple PCs to be installed as a CCASS Terminal to the host computer of HKSCC at the Participant's office premises or its Settlement Agent's office premises located in Hong Kong or in a foreign jurisdiction.

With the exception of Investor Participants, each Participant or its Settlement Agent, in addition to the requirement set out in Section 3.1.1 above, may also be directly linked to CCASS via dedicated data communication links through the installation of a Participant Gateway to the host computer of HKSCC at the Participant's office premises or its Settlement Agent's office premises located in Hong Kong.

All Designated Banks are also required to install CCASS Terminals. In addition, a Designated Bank may also be directly linked to CCASS via dedicated data communication links through the installation of a Participant Gateway to the host computer of HKSCC at the Designated Bank's office premises located in Hong Kong (see Section 3.9). Designated Banks are responsible for bearing their own costs relating to their CCASS Terminals and Participant Gateways (whether in respect of installation, maintenance, connection or otherwise).

Unless otherwise approved by HKSCC, Investor Participants are not entitled to install CCASS Terminals or Participant Gateways. They may access CCASS via the CCASS Phone System using a touch-tone phone, via the CCASS Internet System, or at the Customer Service Centre.

3.1.2 Repealed

3.1.3 Technical requirements

The technical requirements for interface with the CCASS host computer of HKSCC are contained in the CCASS Terminal User Guide for Participants and the CCASS Terminal User Guide for Designated Banks, which can be obtained from HKSCC.

3.1.4 Participants responsible for costs etc.

Participants are responsible for obtaining their own PCs and printers; and for arranging the installation of the required data communication links with CCASS. Participants are also responsible for all costs (maintenance or otherwise) relating to their CCASS Terminals, Participant Gateways, printers, data communication links and related peripherals, as well as for all costs (maintenance or otherwise) relating to the required system software.

3.2 COMMISSIONING OF CCASS TERMINALS AND PARTICIPANT GATEWAYS

3.2.1 Commissioning

Participants and Designated Banks must apply in the prescribed manner to HKSCC for the installation of a CCASS Terminal. Participants and Designated Banks who wish to install a Participant Gateway in addition to a CCASS Terminal must also apply in the prescribed manner to HKSCC.

Participants and Designated Banks may install a CCASS Terminal by themselves or engage service vendors from time to time appointed by HKSCC to install a CCASS Terminal for them. Participants and Designated Banks who wish to install a Participant Gateway should engage service vendors to provide the relevant installation services at their own cost and expense.

The application for and the installation of CCASS Terminals and Participant Gateways shall be subject to such conditions and requirements as HKSCC may from time to time prescribe.

3.2.2 Number and location of CCASS Terminals and Participant Gateways

HKSCC reserves the right to limit the number of CCASS Terminals or Participant Gateways that may be set up or operated by a Participant, its Settlement Agent or a Designated Bank.

A Participant who wishes to install an additional CCASS Terminal or an additional Participant Gateway at a location other than the office premises of the Participant or the office premises of its Settlement Agent must, pursuant to Rule 704, obtain HKSCC's prior written consent to do so. Where consent is granted, installation will be subject to such conditions as prescribed by HKSCC from time to time.

In order for a Participant, a Settlement Agent or a Designated Bank to share CCASS Terminals and Participant Gateways with other Participants, Settlement Agents or Designated Banks, it must first apply to HKSCC in writing and comply with such application procedures as may from time to time be prescribed by HKSCC. Approval of an application to share CCASS Terminals or Participant Gateways is entirely at the discretion of HKSCC. HKSCC may impose such conditions on the sharing arrangement as it thinks fit, whether at the time of approval of the application or at any other time or times thereafter by giving written notice to the Participant, the Settlement Agent or the Designated Bank, as the case may be. HKSCC shall be entitled to revoke any approval granted to a Participant, a Settlement Agent or a Designated Bank concerning its sharing arrangement and discontinue such arrangement at any time by notifying the Participant, the Settlement Agent or the Designated Bank, as the case may be, in writing. HKSCC reserves the right to limit a Settlement Agent's access to the services of CCASS in the event that the Settlement Agent and the Participant who appoints it are operating or accessing the CCASS Terminal or the Participant Gateway simultaneously.

3.2.3 Repealed

3.2.4 Re-commissioning

The re-commissioning of a CCASS Terminal or a Participant Gateway is subject to HKSCC's approval and if approval is given, will be allowed or undertaken at the expense of the Participant or Designated Bank, as the case may be.

3.3 DELEGATED ADMINISTRATORS

3.3.1 Establishing and Cancelling Delegated Administrators

Each Participant must appoint its own administrators ("Delegated Administrators") to

establish or cancel, via CCASS Terminal, the access of its Authorised Users to CCASS.

To appoint and cancel the appointment of a Delegated Administrator, a Participant must apply in the prescribed manner to HKSCC.

Upon approval of an application of a Participant to appoint a Delegated Administrator, HKSCC will provide to the Participant concerned a unique User ID and smartcard, in respect of that Delegated Administrator for access control purposes. The Participant must ensure that its Delegated Administrator creates or changes his initial Smartcard Password (where applicable) immediately upon receipt of the smartcard. If a Delegated Administrator forgets his Smartcard Password, the Participant will need to apply in the prescribed manner to HKSCC to establish a new Smartcard Password.

3.4 AUTHORISED USERS

3.4.1 Establishing and cancelling Authorised Users

Each Participant must ensure that only persons approved as its Authorised Users are allowed access to CCASS via CCASS Terminals.

Each Participant will need to establish or cancel its Authorised Users through its Delegated Administrators via CCASS Terminals.

To establish a new Authorised User, a Participant will need to apply in the prescribed manner to HKSCC for a smartcard for that Authorised User for access control purposes. The Participant must ensure that its new Authorised User creates his initial Smartcard Password or changes his initial Smartcard Password (where applicable) immediately upon receipt of the smartcard.

A Participant will need to establish a new Smartcard Password through its Delegated Administrators via CCASS Terminal for any Authorised User who forgets his Smartcard Password.

3.4A SSA STATEMENT RECIPIENTS

3.4A.1 Maintaining SSA Statement Recipients

Upon the opening of a SSA with Statement Service in CCASS by a Clearing Participant or a Custodian Participant, the Participant must, in respect of that SSA with Statement Service, name and maintain at all times a single SSA Statement Recipient which may comprise an individual, joint individuals, partnerships and/or bodies corporate through the account maintenance functions available via its CCASS Terminal or Participant Gateway. For the avoidance of doubt, the Participant can only name and/or maintain a single SSA Statement Recipient in respect of each SSA with Statement Service. By naming and/or maintaining such SSA Statement Recipient, the Participant authorizes HKSCC to do each of the following in respect of the SSA with Statement Service subject to the Rules and on such terms and conditions as HKSCC may from time to time specify until the SSA with Statement

Service is closed in accordance with the Rules:

- (i) furnish the SSA Statement Recipient with advices, statements and reports relating to the SSA with Statement Service, as referred to in Section 16.8;
- (ii) allow the SSA Statement Recipient to access, via the CCASS Phone System and CCASS Internet System, the enquiry functions in relation to the SSA with Statement Service as referred to in Section 15 and the maintenance functions in relation to the SSA with Statement Service as specified by HKSCC from time to time;
- (iii) send or cause to send messages relating to the stock movements, STI Transfers and voting activities in respect of Eligible Securities in the SSA with Statement Service, and the change in the details of SSA Statement Recipient to the SSA Statement Recipient via the E-mail and/or SMS, as referred to in Section 16.8; and
- (iv) where the Clearing Participant or Custodian Participant has indicated to HKSCC, in such manner as HKSCC may from time to time prescribe, that the SSA Statement Recipient is authorised to give affirmation to STI and/or voting instructions to HKSCC in relation to the SSA with Statement Service for the account of the Participant, to accept and rely on the STI affirmations and/or voting instructions of the SSA Statement Recipient for the account of the Participant as if they were the affirmations or instructions of the Participant.

Provided that the Participant may effect any change of such SSA Statement Recipient named or maintained by it and/or effect any change of the details of such SSA Statement Recipient, both through the account maintenance functions available via CCASS Terminals or Participant Gateways.

If the Clearing Participant or Custodian Participant wishes to delete the SSA Statement Recipient named and/or maintained in respect of a SSA with Statement Service and not to name or maintain another SSA Statement Recipient in respect of that SSA with Statement Service, the Participant must do so by closing the SSA with Statement Service through the account maintenance functions available via CCASS Terminals or Participant Gateways.

Once a SSA with Statement Service is closed, the naming and maintenance of SSA Statement Recipient in respect of that SSA with Statement Service by a Clearing Participant or a Custodian Participant will be cancelled and the authorization given by the Participant to HKSCC in relation to the SSA with Statement Service and the related SSA Statement Recipient will be withdrawn without prejudice to the rights of HKSCC under the Rules. For the avoidance of doubt, HKSCC will not furnish statements relating to the closed SSA with Statement Service to the SSA Statement Recipient, allow the SSA Statement Recipient to access the closed SSA with Statement Service and send E-mail and SMS relating to the closed SSA with Statement Service to the SSA Statement Recipient.

In relation to each of the acts which HKSCC is authorized by a Clearing Participant or a Custodian Participant to do under Section 3.4A.1(i) – (iv) subject to the Rules, HKSCC may from time to time specify the applicable terms and conditions. The Clearing Participant or Custodian Participant shall furnish its SSA Statement Recipients and the person or persons comprising such SSA Statement Recipients with the applicable Rules and such terms and conditions. The Clearing Participant or Custodian Participant shall ensure and shall procure that its SSA Statement Recipients and any person or persons comprising such SSA Statement Recipients comply with the applicable Rules and such terms and conditions.

3.5 ACCESS CONTROL

3.5.1 Logging on to CCASS

In order to log on to CCASS via a CCASS Terminal, an Authorised User or a Delegated Administrator must :

- (i) insert his smartcard into the smartcard reader of the CCASS Terminal; and
- (ii) enter his Smartcard Password into the CCASS Terminal.

Each smartcard provided by HKSCC is unique to the Authorised User or Delegated Administrator to whom it is issued. The identity of an Authorised User or a Delegated Administrator logging on to CCASS will be determined by HKSCC by reference to the smartcard used.

Participants may apply to HKSCC for smartcard readers for their CCASS Terminals in the manner as specified in the CCASS Terminal User Guide and CCASS Terminal User Guide for Designated Banks.

In the event that an Authorised User is unsuccessful in logging on to CCASS via a CCASS Terminal after three attempts, the Participant concerned will need to re-establish that person as an Authorised User through its Delegated Administrator via a CCASS Terminal.

In the event that a Delegated Administrator of a Participant is unsuccessful in logging on to CCASS via a CCASS Terminal after three attempts, the Participant concerned will need to re-establish that person as a Delegated Administrator by applying in the prescribed manner to HKSCC.

In order to log on to CCASS via a Participant Gateway, an Authorised User of a Participant must:

- (i) insert the Participant Gateway smartcard of that Participant into the smartcard reader of the Participant Gateway; and
- (ii) enter the Participant Gateway Smartcard Password of that Participant into the Participant Gateway.

Each Participant Gateway smartcard provided by HKSCC is unique to the Participant to

whom it is issued. The identity of a Participant logging on to CCASS via a Participant Gateway will be determined by HKSCC by reference to the Participant Gateway smartcard used.

Participants may apply to HKSCC for smartcard readers for their Participant Gateways in the manner as specified in the CCASS Terminal User Guide.

In the event that a Participant is unsuccessful in logging on to CCASS via a Participant Gateway after three attempts, the Participant concerned will need to re-establish its access to the Participant Gateway through its Delegated Administrator via a CCASS Terminal.

3.5.2 Administration Rights of a Delegated Administrator

The security management functions to which a Delegated Administrator can access are determined by the Administration Rights specified by a Participant.

A Delegated Administrator will be denied access to security management functions which is not included in the Administration Rights.

At the time of establishing a Delegated Administrator, a Participant will need to determine the Administration Rights for that Delegated Administrator. A Participant may alter the Administration Rights of its Delegated Administrator at any time by applying in the prescribed manner to HKSCC.

3.5.3 Access Level of an Authorised User

The extent to which a particular Authorised User of a Participant can access CCASS functions or services via a CCASS Terminal is determined by the Access Level specified by the Participant for that Authorised User.

An Authorised User of a Participant accessing CCASS via a CCASS Terminal will be denied access to CCASS functions or services for which he is not authorised.

At the time of establishing an Authorised User, a Participant will need to determine the relevant Access Level for that Authorised User. There will be pre-determined Access Levels for a Participant to select for each of its Authorised Users.

A Participant may alter the Access Level of its Authorised Users at any time through its Delegated Administrator via a CCASS Terminal.

3.5.4 Input Transaction Limit of an Authorised User

The extent to which a particular Authorised User of a Participant can input via a CCASS Terminal certain instructions (other than Electronic Application Instructions for New Issue Shares and Tender Instructions) into CCASS will be determined by the Input Transaction Limit (if any) specified by the Participant for that Authorised User.

Instructions which can be made subject to Input Transaction Limits are :

- (i) Account Transfer Instructions or ATIs;
- (ii) Settlement Instructions or SIs;
- (iii) Delivery Instructions or DIs;
- (iv) instructions relating to "Change DI Requirement" function (see Section 13.2.3);
- (v) Investor Settlement Instructions or ISIs;
- (vi) Input Recall Request;
- (vii) Change Cash Compensation Indicator; and
- (viii) Cash Prepayment Instructions.

Save in the case of SIs, ISIs and Cash Prepayment Instructions, instructions input into CCASS by an Authorised User of a Participant via a CCASS Terminal which exceed his Input Transaction Limit will not be entertained by HKSCC. If an SI, ISI or Cash Prepayment Instruction input into CCASS by an Authorised User of a Participant via a CCASS Terminal exceeds his Input Transaction Limit, the respective instruction will remain pending the authorisation of another Authorised User of the Participant with the necessary Input Transaction Limit. In general, the value of the Eligible Securities which are subject to instructions input into CCASS via a CCASS Terminal by an Authorised User will be compared with any Input Transaction Limit applicable to him. For further details, please see the CCASS Terminal User Guide.

A Participant may alter the Input Transaction Limits of its Authorised Users at any time through its Delegated Administrator via a CCASS Terminal.

3.5.5 Participants responsible for security

It is the responsibility of each Participant to control access to its CCASS Terminals, Participant Gateways and to its smartcards to ensure the security and confidentiality of the User IDs and Smartcard Passwords of its Authorised Users and Delegated Administrators and its Participant Gateway Smartcard Password, to ensure that its Authorised Users abide by the Access Levels and Input Transaction Limits assigned to each of them, to ensure the security and confidentiality of the Authorisation Code of its Delegated Administrators, and to ensure that its Delegated Administrators abide by the Administrator Rights assigned to them.

A Participant shall immediately notify HKSCC to disable the user profile associated with a smartcard by submitting the prescribed form to HKSCC if it becomes aware that the smartcard is lost or has been stolen.

Participants shall be liable for all instructions input into CCASS via their CCASS Terminals or Participant Gateways. Participants requiring a new smartcard or a replacement smartcard must complete the prescribed Smartcard Request Form and submit the same to HKSCC. Participants are required to pay the appropriate fees for issuance or replacement of a smartcard (see Section 21.8).

3.6 OPERATIONS UNDERTAKEN THROUGH CCASS TERMINALS AND PARTICIPANT GATEWAYS

The operations that may be undertaken using CCASS Terminals and the procedural steps for executing those operations are set out in the CCASS Terminal User Guide.

The CCASS Terminal User Guide will be updated from time to time to reflect any changes and alterations to the operations that may be undertaken using CCASS Terminals or to the procedural steps for executing those operations.

The operations that may be undertaken using Participant Gateways and the procedural steps for executing those operations are available at the discretion of HKSCC.

3.7 SERVICING OF CCASS TERMINALS AND PARTICIPANT GATEWAYS

Participants requiring assistance relating to the use of CCASS Terminals and Participant Gateways may telephone HKSCC for assistance.

General enquiries should be made using the "CCASS hotline", and enquiries of a technical nature should be made using the "CCASS technical hotline". The telephone numbers and service hours of these hotlines are set out in the CCASS Terminal User Guide and the CCASS Terminal User Guide for Designated Banks.

3.8 BACK-UP CENTRE FOR CCASS TERMINALS

If a Participant's CCASS Terminal breaks down, it will be able to utilise the Back-Up Centre provided by HKSCC.

3.9 CCASS TERMINALS AND PARTICIPANT GATEWAYS OF DESIGNATED BANKS

Designated Banks of all Participants must be electronically linked to the CCASS host computer through a CCASS Terminal for the purpose of informing HKSCC of:

- (i) the payment status of DDIs, DCIs and EPIs affecting Participants other than Investor Participants for whom they act; and
- (ii) the payment status of DDIs and debit EPIs affecting Investor Participants for whom they act.

Designated Banks may also be electronically linked to the CCASS host computer through a Participant Gateway.

Sections 3.1 to 3.4 and Sections 3.5 to 3.8 (with the exception of references to the Input Transaction Limit, which do not apply to Authorised Users of Designated Banks) apply also to the CCASS Terminals and Participant Gateways of Designated Banks.

Designated Banks will use their CCASS Terminals for the purpose of giving or issuing to HKSCC (i) “payment confirmation” as defined in Section 14.4.3(ii); and (ii) “payment confirmation” as defined in Section 14.5.3(i).

Relevant control reports relating to the payments made, received or effected, or to be made, received or effected by Participants for whom a Designated Bank acts can also be retrieved from its CCASS Terminal and Participant Gateway. For further details, please refer to Section 14 and the CCASS Terminal User Guide for Designated Banks.

In addition, Designated Banks can retrieve Electronic CHATS Payment Instruction Reports generated by CCASS from their CCASS Terminals and Participant Gateways. Designated Banks can, based on such Electronic CHATS Payment Instruction Reports, effect CHATS payments on behalf of Participants in respect of money settlement obligations of such Participants in CCASS. For further details, please refer to Section 14 and the CCASS Terminal User Guide for Designated Banks.

Designated Banks can also use their CCASS Terminals and Participant Gateways to access the “Enquire Broadcast Message” function and retrieve reports and statements. For further details, please refer to Sections 15 and 16 and the CCASS Terminal Guide for Designated Banks.

3.10 CCASS PHONE SYSTEM AND CCASS INTERNET SYSTEM

3.10.1 CCASS Phone System and CCASS Internet System available for Investor Participants and SSA Statement Recipients

Once a stock account is opened, an Investor Participant can operate its Stock Account, give instructions on corporate activities, give Electronic Application Instructions for New Issue Shares, Tender Instructions, input ISIs, affirm ISIs, enquire stock balance and input activities via the CCASS Phone System by using a touch-tone phone or at the Customer Service Centre. In addition, an Investor Participant using services available via the CCASS Internet System can give on-line instructions on corporate activities, give Electronic Application Instructions for New Issue Shares, Tender Instructions, input ISIs, affirm ISIs, enquire stock balance and input activities, receive notices and statements. Transfer Instructions must be submitted by the Investor Participant to the Customer Service Centre using the Transfer Instruction Form.

Once a SSA with Statement Service is opened by a Clearing Participant or a Custodian Participant and SSA Statement Recipient in respect of the SSA with Statement Service is named and/or maintained by that Participant, the SSA Statement Recipient can enquire stock balance and stock movement activities in respect of the SSA with Statement Service via the CCASS Phone System by using a touch-tone phone. In addition, such SSA Statement Recipient using services available via the CCASS Internet System can enquire stock balance and stock movement activities in respect of the SSA with Statement Service, and receive advices, statements and reports relating to that SSA with Statement Service.

Where the Clearing Participant or Custodian Participant naming and/or maintaining a SSA Statement Recipient has indicated to HKSCC through the account maintenance function that the SSA Statement Recipient is authorised by the Participant to affirm STI in respect of the SSA with Statement Service and/or to give instruction in relation to actions affecting Eligible Securities in the SSA with Statement Service that are to be voted upon for the account of the Participant, the SSA Statement Recipient may affirm STI and/or give voting instructions in respect of the SSA with Statement Service for the account of the Participant

via the CCASS Phone System by using a touch-tone phone and via the CCASS Internet System.

3.10.2 CCASS Phone User ID and CCASS Phone Password for accessing CCASS Phone System; e-Certificates and Internet User ID and Internet User Password for accessing CCASS Internet System

Upon approval of an application to become an Investor Participant, HKSCC will provide to the Individual Investor Participant or each individual member of the Joint Individual Investor Participant concerned for access to CCASS via the CCASS Phone System:

- (i) a unique CCASS Phone User ID; and
- (ii) an initial CCASS Phone Password.

For a Corporate Investor Participant, the Participant must ensure that only persons approved as its Authorised Users are allowed to operate its Stock Account in CCASS. HKSCC will provide to each of the Authorised Users of a Corporate Investor Participant a unique CCASS Phone User ID and an initial CCASS Phone Password. A Corporate Investor Participant may appoint a maximum of six Authorised Users. To establish or cancel an Authorised User, a Corporate Investor Participant must apply in prescribed manner to HKSCC. Individual and Joint Individual Investor Participant are not allowed to appoint other persons to access CCASS on their behalf.

The CCASS Phone User ID and CCASS Phone Password are personal to an Individual Investor Participant or an individual member of a Joint Individual Investor Participant or an Authorized User of a Corporate Investor Participant for access control purposes.

An Individual Investor Participant, an individual member of a Joint Individual Investor Participant or an Authorised User of a Corporate Investor Participant who has been provided with a unique CCASS Phone User ID and an initial CCASS Phone Password by HKSCC shall, if he wishes to access CCASS via the CCASS Internet System, (i) register a unique set of Internet User ID and Internet User Password with HKSCC; and/or (ii) apply to Hongkong Post for a digital certificate (the "Hongkong Post e-Cert") and then register his Hongkong Post e-Cert with HKSCC. Such individual or Authorised User shall use his CCASS Phone User ID and, if required, CCASS Phone Password to register such Hong Kong Post e-Cert and Internet User ID and Internet User Password.

An Investor Participant agrees that the Internet User ID and Internet User Password are personal to the relevant Individual Investor Participant, individual member of a Joint Individual Investor Participant or Authorised User of a Corporate Investor Participant (as the case may be) for access control purposes.

Upon the opening of a SSA with Statement Service by a Clearing Participant or a Custodian Participant and the naming and/or maintenance of SSA Statement Recipient in respect of the SSA with Statement Service by that Participant, HKSCC will provide a unique CCASS Phone User ID of the SSA with Statement Service to the SSA Statement Recipient via the Participant and the Participant shall provide an initial CCASS Phone Password to the SSA

Statement Recipient for access to the SSA with Statement Service in CCASS via the CCASS Phone System.

The CCASS Phone User ID and the CCASS Phone Password are personal to the SSA Statement Recipient of the Participant for access control purposes.

The SSA Statement Recipient that has been provided with a unique CCASS Phone User ID of the SSA with Statement Service by HKSCC via the Clearing Participant or Custodian Participant and an initial CCASS Phone Password by the Participant shall, if the SSA Statement Recipient wishes to access the SSA with Statement Service in CCASS via the CCASS Internet System, register a unique set of Internet User ID and Internet User Password with HKSCC.

The Clearing Participant or Custodian Participant that has named and/or maintained SSA Statement Recipient in respect of its SSA with Statement Service in CCASS agrees that the Internet User ID and Internet User Password are personal to the SSA Statement Recipient for access control purposes.

3.10.3 Input Transaction Limit of an Authorized User of a Corporate Investor Participant

The extent to which a particular Authorised User of a Corporate Investor Participant can input or affirm an ISI in CCASS will be determined by the Input Transaction Limit specified by the Corporate Investor Participant for that Authorised User. ISI input or affirmed in CCASS by an Authorised User of a Corporate Investor Participant which exceeded his Input Transaction Limit will remain pending for authorisation by another Authorized User of the Corporate Investor Participant with the necessary Input Transaction Limit. In general the value of the Eligible Securities which are subject to instructions input into CCASS by an Authorised User will be compared with the Input Transaction Limit applicable to him. A Corporate Investor Participant may alter the Input Transaction Limit of its Authorised Users at any time by applying in the prescribed manner to HKSCC.

3.10.3A Access to SSA with Statement Service by SSA Statement Recipient

The Clearing Participant or Custodian Participant must ensure that only the SSA Statement Recipient named and/or maintained by the Participant in respect of its SSA with Statement Service is allowed access to the SSA with Statement Service in CCASS via the CCASS Phone System and CCASS Internet System. The Participant is also responsible to ensure that the SSA Statement Recipient and each person comprising such SSA Statement Recipient complies with the terms and conditions prescribed by HKSCC from time to time in relation to such access, including but not limited to the terms of use of the CCASS Internet System, the E-mail and the SMS.

3.10.4 Participants responsible for security

It is the responsibility of each Individual Participant and each individual member of a Joint Individual Investor Participant to ensure the security and confidentiality of its CCASS Phone User ID, CCASS Phone Password, Internet User ID and Internet User Password and password of his Hongkong Post e-Cert. Each such user must ensure that the initial CCASS Phone Password be changed immediately upon receipt.

It is the responsibility of each Corporate Investor Participant to ensure the security and confidentiality of the CCASS Phone User IDs, CCASS Phone Passwords, Internet User IDs

and Internet User Passwords and passwords of the Hongkong Post e-Cert of its Authorized Users, and to ensure that its Authorized Users abide by the Input Transaction Limit assigned to them.

It is the responsibility of each Clearing Participant or Custodian Participant to ensure the security and confidentiality of the CCASS Phone User IDs of the SSA with Statement Service, CCASS Phone Passwords, Internet User IDs and Internet User Passwords provided to or registered by its SSA Statement Recipients, and to ensure that its SSA Statement Recipients and the persons comprising such SSA Statement Recipients abide by the related terms and conditions of use.

As the relevant CCASS Phone Password is unknown to HKSCC, if an Individual Investor Participant or Joint Individual Investor Participant or an Authorized User of a Corporate Investor Participant forgets his CCASS Phone Password or fails to log on to the CCASS Phone System after three attempts, the Investor Participant will need to apply in the prescribed manner to HKSCC to establish a new CCASS Phone Password. If the SSA Statement Recipient forgets the CCASS Phone Password provided to it by the Clearing Participant or Custodian Participant or fails to log on to the CCASS Phone System after three attempts, the Clearing Participant or Custodian Participant concerned will need to establish a new CCASS Phone Password for such SSA Statement Recipient.

Similarly, if an Individual Investor Participant or an individual member of a Joint Individual Investor Participant or an Authorized User of a Corporate Investor Participant forgets his Internet User Password or fails to log on to the CCASS Internet System after three attempts, he will need to apply in the prescribed manner to HKSCC to establish a new Internet User Password. If the SSA Statement Recipient forgets the Internet User Password registered by it or fails to log on to the CCASS Internet System after three attempts, the SSA Statement Recipient will need to establish a new Internet User Password in the prescribed manner specified by HKSCC.

An Investor Participant shall immediately revoke its Hongkong Post e-Cert by using the on-line revoke function of the CCASS Internet System or by submitting the prescribed form to the Customer Service Centre if it becomes aware that its Hongkong Post e-Cert is lost or has been stolen or otherwise compromised. If the revoke obligations set out above are not complied with properly or at all, then HKSCC accepts no liability for any consequences, especially not for any loss or damage that may result to the Investor Participant or any other person.

If an Investor Participant wishes to resume usage of its Hongkong Post e-Cert which was lost and subsequently found, the Investor Participant must apply to HKSCC by using HKSCC's prescribed form.

Investor Participants shall be liable for all instructions input into CCASS. Clearing Participants and Custodian Participants shall be liable for all acts and omissions of their SSA Statement Recipients and of the persons comprising such SSA Statement Recipients.