Introduction

SCSL's (Steel City Securities Limited) intentions for publishing a security Policy are not to impose restrictions that are contrary to SCSL's established culture of openness, trust-worthy and integrity. SCSL is committed to protecting SCSL's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of SCSL. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every SCSL employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose of the Policy

The purpose of this policy is to outline the acceptable use of computer equipment at SCSL. These rules are in place to protect the employee and SCSL. Inappropriate use exposes SCSL to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope of the policy

This policy applies to employees, contractors, consultants, temporaries, and other workers at SCSL, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by SCSL.

General Use and Ownership

While SCSL's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of SCSL. Because of the need to protect SCSL's network, management cannot guarantee the confidentiality of information stored on any network device belonging to SCSL.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies,

employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

It is recommended that any information that users consider sensitive or vulnerable be encrypted.

The software for such work can be winzip or similar software which allow password protection of compressed files

For security and network maintenance purposes, authorized individuals within SCSL may monitor equipment, systems and network traffic at any time.

SCSL reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed Monthly, user level passwords should be changed every three months.

Folder level security should be enforced in cases where it is unavoidable to restrict sharing of folders

All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.

Use encryption of information in compliance with SCSL's acceptable Encryption Use policy.

Because information contained on portable computers is especially vulnerable, special care should be exercised.

Postings by employees from a SCSL email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SCSL, unless the posting is in the course of business duties.

All hosts used by the employee that are connected to the SCSL Internet/Intranet/Extranet, whether owned by the employee or SCSL, shall be continually executing approved virus-scanning software with a current virus database, unless overridden by departmental or group policy.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Restrictions

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of SCSL authorized to engage in any activity that is illegal under local, state, central or international law while utilizing SCSL-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SCSL.

Unauthorized copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SCSL or the end user does not have an active license is strictly prohibited.

Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
Introduction of malicious programs into the network or Server(e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Making fraudulent offers of products, items, or services originating from any SCSL account.

Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

Effecting security is breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Port scanning or security scanning is expressly prohibited unless prior notification to SCSL is made.

Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
Circumventing user authentication or security of any host, network or account.

Interfering with or denying service to any user (for example, denial of service attack).

Anyone doing network monitoring, security testing of the network should take permission of the IT department.

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Providing information about, or lists of, SCSL employees to parties outside

Email and Communications Activities

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

Unauthorized use, or forging, of email header information.

Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", or other "pyramid" schemes of any type.

Use of unsolicited email originating from within SCSL's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SCSL or connected via SCSL's network.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action taken by the management.

Policy for Phones & Faxes

A computer which is capable of making a fax connection is not to be allowed to use an analog line for this purpose.

Computers with modems & having telephone lines are a big security risk since they bypass the firewall.

All downloaded material, prior to being introduced into SCSL systems and networks, must have been scanned by an approved anti-virus utility (e.g., Norton Anti-virus Corporate Edition) which has been kept current through regular updates.

Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.

NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

Delete Spam, chain, and other junk email without forwarding, in with SCSL’s Security.

Never download files from unknown or suspicious sources. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

Always scan a floppy diskette from an unknown source for viruses before using it.

Back-up critical data and system configurations on a regular basis and store the data in a safe place.

If lab-testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

Dial-In Access Policy

SCSL employees and authorized third parties (customers, vendors, etc.) can use dial-in connections to gain access to the corporate network. Dial-in access should be strictly controlled, using one-time password authentication

It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to SCSL is not used by non-employees to gain access to company information system resources. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and SCSL are literal extensions of SCSL's corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect SCSL's assets

Password Policy

All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months. The recommended change interval is every month.

User accounts that have system-level privileges granted through group memberships etc. must have a unique password from all other accounts held by that user.

Passwords must not be inserted into email messages or other forms of electronic communication.

All user-level and system-level passwords must conform to the guidelines described below.

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.

- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.

Password Protection Policy

Do not use the same password for SCSL accounts as for other non-SCSL access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various SCSL access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

Do not share SCSL passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential SCSL information.

Don't reveal a password over the phone to ANYONE
Don't reveal a password in an email message
Don't reveal a password to the boss
Don't talk about a password in front of others
Don't hint at the format of a password (e.g., "my family name")
Don't reveal a password on questionnaires or security forms
Don't share a password with family members
Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Internet explorer).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system without encryption.

If an account or password is suspected to have been compromised, report the incident to EDP and change all related passwords.

Password cracking or guessing may be performed on a periodic or random basis by System Administrator or its delegates on permission from SCSL. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Remote access policy

This policy applies to all SCSL employees, contractors, vendors and agents with a SCSL-owned or personally-owned computer or workstation used to connect to the SCSL network. This policy applies to remote access connections used to do work on behalf of SCSL, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

It is the responsibility of SCSL employees, contractors, vendors and agents with remote access privileges to SCSL's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to SCSL.

General access to the Internet by immediate household members through the SCSL Network on personal computers is prohibited. Employee bears responsibility for the consequences should the access be misused.

Requirements

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

At no time should any SCSL employee provide his or her login or email password to anyone, not even family members.

SCSL employees and contractors with remote access privileges must ensure that their SCSL-owned or personal computer or workstation, which is remotely connected to SCSL's corporate network, is not connected to any other network at the same time with the exception of personal networks that are under the complete control of the user.

SCSL employees and contractors with remote access privileges to SCSL's corporate network must not use non-SCSL email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct SCSL business, thereby ensuring that official business is never confused with personal business.

Router Security Policy

The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.

Use corporate standardized SNMP community strings.
Access rules are to be added as business needs arise.
The router must be included in the corporate enterprise management system with a designated point of contact.
Each router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

This above message should be in the router telnet banner also.

Server Security Policy

All internal servers deployed at SCSL, must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by SCSL.

Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by SCSL.

Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

Server contact(s) and location, and a backup contact
Hardware and Operating System/Version
Main functions and applications, if applicable
Information in the corporate enterprise management system must be kept up-to-date.
Configuration changes for production servers must follow the appropriate change management procedures.

Adequate Power Backup systems should be provided to all computers & especially servers to ensure that abnormal shutdowns do not occur & thereby lead to disruption of services. The UPS systems should be regularly monitored & logs maintained.

The servers should be preferably purchased with redundant power supplies and/or the UPS's purchased should be intelligent to signal a planned shutdown of the server attached to it.

General Configuration Guidelines

Operating System configuration should be in accordance with approved guidelines.
Services and applications that will not be used must be disabled where practical.

Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

Always use standard security principles of least required access to perform a function.

Do not use root when a non-privileged account will do.

If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed only over secure channels, (e.g., encrypted network connections using SSH or IPSec).

Servers should be physically located in an access-controlled environment. Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

All security related logs will be kept online for a minimum of 1 week.
Daily incremental tape backups will be retained for at least 1 month.
Weekly full tape backups of logs will be retained for at least 1 month.
Monthly full backups will be retained for a minimum of 2 years.
Security-related events will be reported to System Administrator, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed.

Security-related events include, but are not limited to:
Port-scan attacks
Evidence of unauthorized access to privileged accounts
Anomalous occurrences that are not related to specific applications on the host.

Backup and Disaster Recovery:

In spite of reliable hardware, software and administration, there are times when systems crash or fail. The failure may be due to hacking also. Always good system administration involves reliable backup and recovery procedure. Depending upon the business need, you have to plan backup procedures. You may use built-in backup and recovery tools in the

Operating System or dedicated software from a different vender. Some times you may require, an additional hardware for backing up the data.

Some of the important facts to consider while planning backup are,

How frequently you have to back up data and what is the best time to backup
How much data to be backed up
Off-site storage of the data in case of catastrophe
How long the backup data to be stored
Security of the backup data: Backup media should be stored in a secured place. If the data is stored on-line, securing the data from a hacker/intruder is equally important.
Good documentation for backup and recovery procedure

Many of the considerations depend upon the business need and the corporate goal. Any backup and disaster recovery plan/procedure is not complete unless it is tested.

Periodically you have to test if the data recovery is working. When you are planning for backup and disaster recovery, basic rules are, how fast you have to rebuild the system to the latest working state, if the entire system is destroyed and how much data you can afford to lose.

Additional Note

When systems have to be redistributed by way of exchange from one user to another user or have to be temporarily supplied for a specific project to various departments on an ad-hoc basis, the existing data on those systems has to be totally deleted or the entire hard disk should be formatted before allotment/exchange of such systems.

Introduction

SCSL's (Steel City Securities Limited) intentions for publishing a policy on Clearing and Settlement are not to impose restrictions that are contrary to SCSL's established culture of openness, trust-worthy and integrity. SCSL is strictly following Rules/Regulations/Bye-Laws of SEBI and Exchanges to facilitate a Trading platform to transact with more transparency and to maintain a good business relationship with Clients, Individual Investors and Business associates.

We are providing Exchanges connectivity via VSAT and Internet to access the Market Watch of different Exchanges and Segments. Trader Work Stations are being installed to place their Buy/Sell orders, Price Enquiry, Confirmations, Outstanding Position, Net Positions, Funds and Securities.

Effective service and monitoring is a team effort involving the participation and support of every SCSL employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

Purpose of the Policy

The purpose of this policy is to outline the business operations and not to deviate from the procedures being followed at SCSL. These procedures are in place to protect the Clients, Investors and SCSL. Inappropriate application of these procedures exposes SCSL to risks including disablement by SEBI/Exchange, Loosing Market Good will, Financial Loss and legal issues.

Scope of Policy

This policy applies to employees, Clients, Investors, Sub-brokers, and other Business associates at SCSL. This policy also applies to all business activities those are performed through SCSL.

Client Registration Policy

KYC is the key-document to assess the person who desires to associate with SCSL to avail a business platform. SCSL is very keen on certifying/identifying the authenticity of any person dealing with financial markets in any segment. We have to strictly follow the in-person verification before signing of any undertaking/agreement to avoid illegal activities.

The KYC document is being filled by the individual/corporate with all relevant details and not leaving anything undisclosed. The information is being declared in KYC is carrying a validity to prosecute any illegal/unauthorized issues in future. This vital document is preserved in good manner to recall for any verification or audits at any time.

The supporting document of KYC is to strengthen the profile of individual/corporate and to comply with the SEBI/Exchanges guidelines. These supporting documents like PAN, Address Proof, Latest Bank Statement and Proof of identity, Memorandum of Articles, Board resolution, Networth Certificate are mandatory to furnish while registering as an individual/corporate. And these details can not be modified unless otherwise it is requested in writing by the individual/corporate.

Maker and checker is to ensure the genuineness of the document in all aspects to certify the information for successful acceptance for registration process. This exercise is mandatory and can not be over ruled.

The registration details have to be uploaded to the respective Exchanges to obtain the prior approval before commencement of business transaction wit us.

As per SEBI/Exchange mandatory, the copy of registered document of KYC along with Welcome letter is to be delivered with in 7 working days.

Closure of Account Policy

The account closing process is initiated based on the intension of account holder only. Before closing the account, SCSL has to obtain the account closure letter with complete details of the account holder. The concerned dept. manager/head has to be approved for processing of the closure of account. All outstanding balances of funds and securities are to be transferred to respective DP and bank account as declared in the account closure letter.

Dealing with in-operated accounts for more than 180 days has to be marked as "DORMANT". These accounts are viewed carefully to avoid unauthorized transactions. The account holder wanted to bring in live after 180 days or so, he/she has to submit the mandatory information to re check/verify the master details of the existing records. After through verification of master details and approval from the concerned dept. Manager/head, the account can be put in live and transaction can be resumed.

Dealing with in-operated accounts for more than 2 years has to be marked as "VERY OLD DORMANT". These accounts are viewed very carefully to avoid unauthorized Dealing with accounts. The account holder wanted to bring in live after 2 years or so, he/she has to re-submit the entire document of KYC and agreements to avoid the invalid/expiry of details. After through verification and approval from the concerned dept. Manager/head, the account can be put in live and transaction can be resumed.

If the account holder is willing to transfer his account to another location of branch or sub-broker, he/she has to submit the request letter to concerned dept. Manager/head at head office to initiate the process. After through reconciliation of out-standing of Funds and securities, the particular account will be transferred and the same will be intimated and recorded at both the parties.

Posting of Reports to clients Policy

As per Exchanges mandatory, SCSL has to send the periodical statements to the ultimate client either in electronically signed or hard copy. The quarterly-ending statement of Funds and Securities will show the history of debit and credit entries during the period.

It is very important to keep the proof of delivery to recall for any future reference or verification in the event of undelivered or lost. These statements are being sent through courier and under certificate of posting whichever services are feasible or available.

Every end of the calendar quarter, clients who have traded and having balances of funds/securities the statements of finance and scrip ledger are being posted to clients address. If client found any error or any wrong reporting, should be informed to SCSL with in 7 working days from the date of receipt.

Weekly ledger balances of funds are sending through SMS to respective clients. This service is being provided to post the latest information to acknowledge instantly without any delay.

Clearing & Settlement System

Clearing and Settlement is a post-trading operation. This process is being followed based on the Exchange Clearing and Settlement cycle for the calendar Year. This is an obligation between the Exchange, Trading Member and the Ultimate Client. SCSL is a intermediary to settle the obligation between Exchange and the ultimate client. As a intermediary, SCSL is having an account called "Pool Account", where all the inward and outward deliveries are being maintained. This pool account holds the information of all traded scrip quantities being transacted on behalf of SCSL.

Settlement System has been designed by the Exchanges to facilitate the realization of Funds and Securities to the beneficiaries account based on their business transactions. SCSL is responsible to complete the settlement obligation of Securities and Funds between the Exchange and the Ultimate Client in time. The client is also having minimum responsibility to meet the obligation as per the settlement cycles.

Security Shortage Policy

The nature of Security shortage is, unable to meet the Exchange Obligation by means of various unexpected reasons by the client. In such cases, the Exchange will recover the shortage by purchasing the shares from the Auction market at prevailing rate. This auction amount will be recovered from the member's account.

Internal Shortage policy

In case of Internal Shortage, selling client is unable to deliver the shares, for various reasons such as short delivery, where another client is having buying position for the same scrip. This obligation will be settled as Internal Shortage at SCSL. In case the buying position is not available at SCSL, SCSL purchases the shortage securities from the exchange at market rate and the same will be transferred to the client's account. The entire process has to be completed in T+3 days.

Auction at Exchange level

In the event of Exchange Auction, the selling position of the trading member is unable to deliver the shares, for some reasons such as short delivery, bad delivery and objections. The exchange purchases the short quantity in the auction market and delivers to the buying position of the trading member. The difference of auction amount either debit or credit will be collected from respective trading member. This process completes in T+5 days.

The following activities are strictly followed with no exceptions:

Whenever client want to open a trading account, we explain our company's profile, brokerage schemes, trading rules and regulation, Know Your Client norms, agreement details, investor rights and obligations and risk discloser details etc.

If client is willing to associate with us, we request client to fulfill and submit all the details with necessary supporting documents.

All these documents will be verified and validated along with the original documents. After strict scrutiny, the concerned authority will stamp and signed on the copies for further process.

PAN details are being verified through an Indian government authorized website www.tin-nsdl.com (Database Source : Income Tax Dept.)

If details are matched through www.tin-nsdl.com , the maker and checker personnel will put a verified stamp on PAN copy and signed. Otherwise entire document will be rejected.

The on-roll employee of SCSL will do the "in-person verification" of client.

After successful in-person-verification, all related documents have to be signed by the designated employee with his name, employee code and designation.

On completion of application in all aspects, UCC is being allotted and created as a new record in master data of back office.

The valid information (UCC details) has to be uploaded to the Exchange.

On successful acceptance from the Exchange, that particular client can be allowed for Normal Trading initial margin.

As per the Exchange mandatory, the Exchange approved UCC (Unique Client Code) details, Copy of KYC and agreements, Pool Account details, User id and Password of ECN (Electronic Contract Note) and /Back-office along with Welcome Letter must be delivered with in 30 working days to respective client address.

The clearing department of SCSL carries out the pay-in and pay-out confirmation process of securities as per settlement calendar of the Exchange. The purpose of this process is to transfer the securities to respective client beneficiary account to Exchanges from the SCSL pool account.

Pay-in of securities: all the shares obligations are picked up from the client's beneficiary account and transferred to SCSL pool account. All transferred shares are being delivered to the National Securities Clearing Corporations Limited (NSCCL) to complete the securities pay-in obligation in time.

Pay-in of funds: payments received from the clients account, are deposited in the SCSL account. These funds will be transferred to NSCCL to complete the funds pay-in obligation in time.

Pay-out of securities: shares are received from the NSCCL and the same is being transferred to SCSL pool account. And further these shares are transferred to the client beneficiary account.

Pay-out of funds: funds received from the NSCCL to SCSL Bank A/c. Immediately the pay-out of funds will be released to client's bank a/c.

Client's gross net positions, from whom we have to receive and to whom we have to deliver (i.e purchases and sales) are available at clearing department.

On T+1 (Trading day plus one) day, the clients those are not transferred their selling quantities to CM Pool a/c, has to be intimated the status of outstanding immediately.

Quantities will be re-delivered to full-fill the selling obligation, only if the client bought in previous settlements or having his/her margin with us

If the client short delivery is identified as an internal shortage, SCSL will purchases the securities from the exchange at market rate and the shares are transferred to the client's account. Internal shortage charges at 1% on value will be debited from default client account and credited to beneficial client account. In case If the securities are not bought in the normal market (if there are no sellers even in the market) they are deemed to closed-out at the highest price between the first day of the trading period till the day of squaring off or 20% greater than the official close price on the close out-day, whichever is higher. This amount is credited to the receiving client 's account and charged to the default client.

The pay-out is being stopped as per undertaking given by the clients to keep their purchased shares in SCSL pool account for the purpose of intra-day margin requirements, otherwise shares are transferred as per Exchange schedule.

As per exchanges list of approved scrips with hair cuts, being considered for margin and uploaded to the respective exchanges to enable for the intra-day trading. Whenever the

client is selling shares against margin scrip, the same amount will be reduced from margin value.

When ever companies have declared book closures/record date for the purpose of corporate benefits, data available with exchange/depository websites has to be posted in the back office.

Client having shares in pool/margin account will be entitled to claim their corporate benefits and same will be transferred to respective trading / demat accounts from time to time within 30 days from the date of receipt of dividend / warrant.

Companies those are not posted their corporate benefits, clearing department should communicate with the company/registrar.

If any un-identified shares received in pool account, SCSL will wait up to 3 months period. Even though the client is not responded, the shares will be transferred to respective same beneficiary accounts.

In case respective client demat account is closed, the status of shares will be remained as un-identified.

Introduction

SCSL's (Steel City Securities Limited) intentions for publishing a policy on Prevention of Anti Money Laundering Act is not to impose restrictions that are contrary to SCSL's established culture of openness, trust-worthy and integrity. SCSL is strictly following Rules/Regulations/Bye-Laws to maintain the compliance of Regularity Authorities/SEBI and Exchanges to facilitate a Trading platform to transact with more transparency and to maintain a good business relationship with Clients, Individual Investors and Business associates.

We are providing Exchanges connectivity via VSAT and Internet to access the Market Watch of different Exchanges and Segments. Trader Work Stations are being installed to place their Buy/Sell orders, Price Enquiry, Confirmations, Outstanding Position, Net Positions, Funds and Securities.

Effective service and monitoring is a team effort involving the participation and support of every SCSL employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

Purpose of the Policy

The purpose of this policy is to outline the business operations and not to deviate from the procedures being followed at SCSL. These procedures are in place to protect the Clients, Investors and SCSL. Inappropriate application of these procedures exposes SCSL to risks including disablement by SEBI/Exchange, Loosing Market Good will, Financial Loss and legal issues.

Scope of the policy

This policy applies to employees, Clients, Investors, Sub-brokers, and other Business associates at SCSL. This policy also applies to all business activities those are performed through SCSL.

Client Due Diligence

Obtaining sufficient information in order to identify persons who beneficially own or control securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Verifying the client's identity using reliable, independent source documents, data or information;

Identifying beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the customer and/or the person on whose behalf a transaction is being conducted;

Verifying the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and

Conducting ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with SCSL's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.

Policy for acceptance of clients:

No account should be opened in a fictitious / benami name or on an anonymous basis.

Factors of risk perception (in terms of monitoring suspicious transactions) of the client's domicile, the nature of activities, and financial capacity must be verified in back-end

process. Based on these parameters, the client should clearly classify as low, medium and high risk. These classifications are to be updated regularly in KYC document.

SCSL should ensure that an account is not opened where it is unable to apply appropriate clients due diligence measures/KYC polices. This may be applicable in cases where it is not possible to ascertain the identity of the client, information provided to the SCSL is suspected to be non genuine, perceived non co-operation of the client in providing full and complete information. SCSL should not allow such client and file a suspicious activity report to determine any suspicious trading. In such cases the account must be free zed or closed. SCSL is more cautious to ensure that it does not return securities of money that may be from suspicious trades. However, SCSL should consult the relevant authorities in determining what action it should take when it suspects suspicious trading.

In case, the client is permitted to act on behalf of another person, the extent of account operation must be keep tracking of transactions, volume limits, exposure limits and the value of transaction exceeding from the actual eligibility/allocation. The role and responsibilities of both the persons must be verified to avoid illegal/malicious trading activities.

The relationship of the client has to be screened and ensure that the identity of the client does not have any links with person having a criminal background.

Risk-based Approach

According to client's background, he may belongs to higher or lower risk category. In such cases, SCSL should apply the client due diligence measures on a risk sensitive basis. According to the risk sensitiveness, SCSL should do in-depth scrutiny as compared to medium and lower risk levels. In line with the risk-based approach, the type and amount of identification information and documents should obtain necessarily depend on the risk category of a particular client.

The following entities are to be verified as a Clients of special category (CSC):

- Non resident clients
- High net-worth clients,
- Trust, Charities, NGOs and organizations receiving donations
- Companies having close family shareholdings or beneficial ownership
- Politically exposed persons (PEP) of foreign origin
- Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
- Companies offering foreign exchange offerings
- Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against

which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.

- Non face to face clients
- Clients with dubious reputation as per public information available etc.

Client identification procedure:

SCSL is very keen on identifying the client's reliability or honesty while maintaining the relationship, behaviour of transactions, payments and other procedural adoptions. The attitude of the client can be measured from the KYC documents.

The supporting documents and agreements of KYC are being maintained with latest amendments as per SEBI/Exchange circulars. And this is also ensured that uniformity of documentation across the multiple Exchanges/Segments. This uniformity is t avoid unrealistic and in compatible information.

In order to further strengthen the KYC norms and identify every associate in the securities market with their respective PAN thereby ensuring sound audit trail of all the transactions, PAN has been made sole identification number for all participants transacting in the securities market, irrespective of the amount of transaction

SCSL does not indulge nor support any political activities or maintaining any relationship anywhere at branch or sub-broker locations

The client should be identified by using reliable sources including documents / information. The SCSL should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the SCSL in compliance with the Guidelines. Each original documents should be seen prior to acceptance of a copy.

Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority of SCSL.

SCSL shall formulate and implement a client identification programme which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records enable it to determine the true identity of clients. A copy of the client identification programme shall be forwarded to the Director, FIU- IND.

It may be noted that while risk based approach may be adopted at the time of establishing business relationship with a client, no exemption from obtaining the minimum information/documents from clients.

Record Keeping

SCSL should ensure compliance with the record keeping requirements contained sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior. To enable this reconstruction, SCSL should retain the following information for the accounts of clients in order to maintain a satisfactory audit trail:

(a) the beneficial owner of the account;
(b) the volume of the funds flowing through the account; and
(c) for selected transactions:
• the origin of the funds;
• the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
• the identity of the person undertaking the transaction;
• the destination of the funds;
• the form of instruction and authority.

SCSL should ensure that all clients and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, they should consider retaining certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

More specifically, SCSL shall put in place a system of maintaining proper record of transactions prescribed under Rule 3, notified under the Prevention of Money Laundering Act (PMLA), 2002 as mentioned below:

(i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency.
(ii) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh.
(iii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place.
(iv) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

Information to be maintained

SCSL have to maintain and preserve the following information in respect of transactions referred to in Rule 3 of PMLA Rules:

I. the nature of the transactions;
II. the amount of the transaction and the currency in which it denominated;
III. the date on which the transaction was conducted; and
IV. the parties to the transaction.

Retention of Records

SCSL should take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PMLA Rules have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and SCSL.

SCSL is required to formulate and implement the client identification program containing the requirements as laid down in Rule 9 and such other additional requirements that it considers appropriate. The records of the identity of clients have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and SCSL.

The following document retention terms should be observed:

All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars.

Records on client identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence should also be kept for the same period.

In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

Role of Principal Officer

SCSL is properly discharging legal obligations to report suspicious transactions to the authorities, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions.

Names, designation and addresses (including e-mail addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU.

As a matter of principle, it is advisable that the 'Principal Officer' is of a sufficiently higher position and is able to discharge his functions with independence and authority.

Monitoring of Transactions

SCSL should pay special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose. SCSL may specify internal threshold limits for each class of client accounts and pay special attention to the transaction which exceeds these limits.

SCSL should ensure a record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority. Suspicious transactions should also be regularly reported to the higher authorities / head of the department.

Further the compliance dept. of SCSL should randomly examine a selection of transaction undertaken by clients to comment on their nature i.e. whether they are in the suspicious transactions or not.

Suspicious Transaction Monitoring & Reporting

SCSL should ensure to take appropriate steps to enable suspicious transactions to be recognised and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, intermediaries should be guided by definition of suspicious transaction contained in PML Rules as amended from time to time.

A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

a) Clients whose identity verification seems difficult or clients appears not to cooperate
b) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
c) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;
d) Substantial increases in business without apparent cause;
e) Unusually large cash deposits made by an individual or business;
f) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
g) Transfer of investment proceeds to apparently unrelated third parties;
h) Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of export-import of small items.

Any suspicion transaction should be immediately notified to the Money Laundering Principal Officer. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

It is likely that in some cases transactions are abandoned/aborted by clients on being asked to give some details or to provide documents. SCSL should ensure to report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

Reporting to Financial Intelligence Unit-India

In terms of the PMLA rules, SCSL is required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021. Website: http://fiuindia.gov.in/

SCSL is carefully going through all the reporting requirements and formats divided into two parts- Manual Formats and Electronic Formats. While detailed instructions for filing all types of reports are given in the instructions part of the related formats and should adhere to the following:

The cash transaction report (CTR) (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month.

The Suspicious Transaction Report (STR) should be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.

The Principal Officer is responsible for timely submission of CTR and STR to FIU-IND;

Utmost confidentiality should be maintained in filing of CTR and STR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.

No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

No restrictions on operations in the accounts where an STR has been made. The directors, officers and employees (permanent and temporary) should be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to

the FIU-IND. Thus, it should be ensured that there is no tipping off to the client at any level.

Hiring of Employees

SCSL is having adequate screening procedures in place to ensure standards when hiring employees. They should identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

Employee's Training

SCSL is having an ongoing employee training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements being focused for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new customers.

SCSL staff is much concerned that understanding the motivation behind these guidelines, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by ruthless elements.

Investors Education

SCSL is in practice of conducting on-going Investor Awareness programs to create awareness among the investors to understand the business entities and their requirements to participate in the market without deviating from the SEBI/Exchanges/Regularities fame work. In regard to AML/CFT, Investor/client has to declare their financial information including source of funds/income tax returns/bank records etc. SCSL is prepared specific literature/ pamphlets etc. so as to educate the customer of the objectives of the AML/CFT programme.

Introduction

SCSL's (Steel City Securities Limited) intentions for publishing a policy on Legal Fame work is not to impose restrictions that are contrary to SCSL's established culture of openness, trust-worthy and integrity. SCSL is strictly following Rules/Regulations/Bye-Laws to maintain the compliance of Regularity Authorities/SEBI and Exchanges to

facilitate a Trading platform to transact with more transparency and to maintain a good business relationship with Clients, Individual Investors and Business associates.

We are providing Exchanges connectivity via VSAT and Internet to access the Market Watch of different Exchanges and Segments. Trader Work Stations are being installed to place their Buy/Sell orders, Price Enquiry, Confirmations, Outstanding Position, Net Positions, Funds and Securities.

Effective service and monitoring is a team effort involving the participation and support of every SCSL employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

Purpose of the Policy

The purpose of this policy is to outline the business operations and not to deviate from the procedures being followed at SCSL. These procedures are in place to protect the Clients, Investors and SCSL. Inappropriate application of these procedures exposes SCSL to risks including disablement by SEBI/Exchange, Loosing Market Good will, Financial Loss and legal issues.

Scope of the policy

This policy applies to employees, Clients, Investors, Sub-brokers, and other Business associates at SCSL. This policy also applies to all business activities those are performed through SCSL.

Legal Verification of documents

SCSL is very keen while scrutinizing the disclosed information of any vetted document for legal verification. If any quarries were found, we suggest our heads of the concerned Branches/Sub-Brokers to incorporate the relevant information to ensure the adequacy of Rules and By-laws of SEBI and Exchanges.

In the legal frame work, all depts. and their functional operations are much protected from the illegal bindings/promises/agreements etc. SCSL is having an exclusive inspection dept. to ensure the correct processes and following the guidelines of SEBI and Exchanges with latest amendments. Periodical and surprise audits are being conducted at Branch and Sub-Broker offices to identify the practices in regular business operations.

Findings of any non-compliance or unauthorized activities in post inspection/audit report, the management will take appropriate action to control on recurrences in future.

SCSL adhere to take stringent action against any defaulter who committed as a default in clearing his/her pay-in dues during his/her business transactions. As a part of recovery of the unpaid amounts, we approach the Arbitration Departments of the concerned Exchanges to resolve the matter and subsequently approach Visakhapatnam Courts as per the jurisdictions of the law. The action will be initiated upon the consent of the Management to maintain strict financial discipline among the clients.

Opening and Closing of Brach/Sub-Broker

Prior to opening a Branch or Sub-Broker, SCSL conducts a detailed survey on proposed location to identify the business potentiality, banking facility, attitude of the clients, trust-worthiness, local market competitiveness, commercial establishments, and Communication facilities. Based on the survey report, Management will take a decision to setup a branch/sub-broker at the proposed location.

In the event of closing a Branch or Sub-Broker's office, SCSL will obtain a formal letter from the concerned Branch/Sub-Broker and explaining reasons for the closing of a particular location. Before closing the business operations, SCSL will inform to all clients and same will be published in the two local newspapers for public awareness.

Transactional issues

In view of the client's business transactional issues, SCSL will conduct an immediate site inspection/audit to enquire about the incident. On thorough verification to the extent possible, the inspection team will submit a final report to the Management. Based on the level of severity, the issue will proceed further to Investor Grievance Cell of the concerned Exchanges. As per the proceedings and findings of the arbitration, issues will be settled in favor of either party.

Insurance coverage

Since the financial markets are prone to volatile, SCSL is having Stock Brokers Indemnity Policy with New India Insurance Company for all national level Exchanges. Basically these policies are protecting the interest of any clients and employees who have committed abnormal/wrong deals unknowingly during the market hours.

Introduction

SCSL's (Steel City Securities Limited) intentions for publishing a Risk Management Policy are not to impose restrictions that are contrary to SCSL's established culture of openness, trust-worthy and integrity. SCSL is strictly following Rules/Regulations/Bye-Laws of SEBI and Exchanges to facilitate a Trading platform to transact with more transparency and to maintain a good business relationship with Clients, Individual Investors and Business associates.

We are providing Exchanges connectivity via VSAT and Internet to access the Market Watch of different Exchanges and Segments. Trader Work Stations are being installed to place their Buy/Sell orders, Price Enquiry, Confirmations, Outstanding Position, Net Positions, Funds and Securities.

Effective service and monitoring is a team effort involving the participation and support of every SCSL employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

Purpose of the Policy

The purpose of this policy is to outline the business operations and not to deviate from the procedures being followed at SCSL. These procedures are in place to protect the Clients, Investors and SCSL. Inappropriate application of these procedures exposes SCSL to risks including disablement by SEBI/Exchange, Loosing Market Good will, Financial Loss and legal issues.

Scope of the policy

This policy applies to employees, Clients, Investors, Sub-brokers, and other Business associates at SCSL. This policy also applies to all business activities those are performed through SCSL.

Pay-in Collection policy

As per the Exchange settlement cycle, we have to collect the pay-in either funds or securities within T+1. If the client is unable to complete the pay-in obligation with in T+2, he/she will not be allowed for fresh buying.

Cycle of Pay-in

Capital Market Segment

T+1 collect from clients
T+2 Morning Completing the Exchange obligation
T+3 Releasing of payout of funds and securities

Future and Options Segment

T+1 collection for client
T+1 Morning completing the Exchange Obligation
T+1 Evening Pay-out from Exchange
T+2 Releasing of Payout to clients

Margin maintenance Policy

We have been maintaining the margin system to protect the client/sub-broker from the risk and unexpected losses. This is purely based on the market conditions and the client's history of maintaining the account with us. SCSL does not allow any client/sub-broker to transact in any Exchange/Segments without margin either in cash or collateral. According to margin availability, we consider the intra-day exposure limits. And these exposure limits are not fixed and will vary based on the market conditions/volatility. In case of Derivative segment, margin has to be maintained as per the Exchange specifications.

SCSL has sending a consolidated margin report on EOD basis to all clients/sub-brokers to know the outstanding position to prepare for the next trading session. This report has been prescribed by the Exchange to inform all clients regularly.

The soft copy is being maintained for intra-day margins calls for any future reference.

Mode of Payment and Receipts (from/to clients) Policy

SCSL is not encouraging the cash transaction while processing the payment and receipts. We accept payment only through Check/DD/Online Transfer. In case of payment through Demand Draft, the payee has to declare the details of the Demand Draft in his covering letter. Do not accept any third-party cheques under any circumstances. This will help us to avoid unrealized/unauthorized dealing of funds.

Square-off Policy

Squaring-off position is being done only in case of unrealized margin outstanding, minimizing the further losses and any unforeseen market conditions. Before squaring-off

any position, we always seek the final opinion from the owner of the transaction in multiple intervals.

In the event of unanswered, irresponsible, intimating/sending messages in multiple intervals and considering the duration of live market session, if the owner of the transaction does not respond in time, the Management/RMS will be the final decision maker to Square-off the position immediately and the same will be intimated to the ultimate client through concerned Branch Manager/Sub-broker.

The value of margin before squaring-off any qty should meet 100%. In other instances up to 75% is also considered based on the client's previous history of transactions.

Internal Controls on RMS Policy

SCSL is having a robust mechanism of internal controls on Risk Management to safe-guard the Clients and Business associates. All tracking, filtering, alarming mechanism is in place to avoid malpractice, suspicious and other unauthorized entries through our system. The level of hierarchy is being maintained to manage the risk parameters.

Corporate ID	Exchange Connectivity
Connect2NSE	Exchange Connectivity
CTCL Surveillance Administration	CTCL vendor Software
Risk Monitoring Software – Deri-Watch	Vendor Software
Access of online Back-office	In-house connectivity
On hand Surveillance reports	MIS reports

Liquidation of client position Policy

Before liquidation of any position, we are seeking a feed-back from the respective branch head or sub-broker on minimizing the risk. In case of severity, the decision will be taken by the management and same will be informed to concerned leads. And all these messages are communicating through telephone/mobile and CTCL Server. The above process is being declared in voluntary document of MCA/KYC/RDD.

Transfer of Trades Policy

The transferring of trades is being done mostly in the case of typographical error while placing the orders by the dealer.

Order receipt and execution Policy

While receiving of orders, that particular client has been verified by obtaining PAN No, UCC and Address.

Proprietary Trade

Our main business focus is towards retail trades only and we have not enrolled for pro-trading with any Exchange/Segments.

Introduction

SCSL's (Steel City Securities Limited) intentions for publishing a policy on Settlement of Funds is not to impose restrictions that are contrary to SCSL's established culture of openness, trust-worthy and integrity. SCSL is strictly following Rules/Regulations/Bye-Laws to maintain the compliance of Regularity Authorities/SEBI and Exchanges to facilitate a Trading platform to transact with more transparency and to maintain a good business relationship with Clients, Individual Investors and Business associates.
We are providing Exchanges connectivity via VSAT and Internet to access the Market Watch of different Exchanges and Segments. Trader Work Stations are being installed to place their Buy/Sell orders, Price Enquiry, Confirmations, Outstanding Position, Net Positions, Funds and Securities.
Effective service and monitoring is a team effort involving the participation and support of every SCSL employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

Purpose of the Policy

The purpose of this policy is to outline the business operations and not to deviate from the procedures being followed at SCSL. These procedures are in place to protect the Clients, Investors and SCSL. Inappropriate application of these procedures exposes SCSL to risks including disablement by SEBI/Exchange, Loosing Market Good will, Financial Loss and legal issues.

Scope of the policy

This policy applies to employees, Clients, Investors, Sub-brokers, and other Business associates at SCSL. This policy also applies to all business activities those are performed through SCSL.

Process of Transactions

After completion of the BackOffice at the end of the day, the data will be ready for posting of journal vouchers in the finance module. The procedure for posting of journal vouchers in the finance module is as follows:

Firstly, we have to check out for the new clients who have done trading for the first time. Those clients are to be created in the Account Master of the Finance Module. This is automatically done and no manual intervention is required. While creating the new clients, if we come across any new branch that has started business on that particular day,

then we have to create the Branch in the Branch Master of the Finance Module and also the groups in the Group Master.

After checking is done for creation of new branch and new clients, we have to dump the data into the Finance Module with the bill dumping process which is a part of the Trading Module. Then automatically the Journal Vouchers are created in the Finance Module, debiting the Client Account and giving Credit to the Temporary Account called CLEARING A/C for the clients who have either bought shares or incurred Loss during the trading. And for those who have sold shares or gained Profit during the trading the Client Account is Credited and the temporary account is debited automatically. During the process of this bill dumping, all the statutory deductions like Service Tax, Statutory Cost, STT, Stamp Duty and the incomes in the form of Brokerage and Delivery Commission earned for the trading day are given credit to their respective Heads of Account in the Finance Module.

Once the process of bill dumping is complete, we have to check for the clients who have debit balance in their obligation account and have a credit balance in their margin account. If any, then we have to pass a journal voucher automatically for those clients adjusting their debit balance to their margin balance.

After completion of the above said process, we have to generate a consolidated file consisting of all the segments and exchanges. The file is generated in csv format and given to the Trading Department for the purpose of margin calculation.

Collection of Pay-in

The Pay In Amount from the clients are to be collected within 24 hours (T + 1) day in the form of Cheques/Demand Draft/Pay Orders. Receiving the Pay In Amount by CASH is strictly prohibited and should not be accepted. The Cheques or Demand Drafts collected from clients towards their Pay In obligation are entered into the Finance Module. The original receipt is handed over to the concerned client and a duplicate is filed for office records. All the collected cheques / demand drafts are deposited into the respective Bank Accounts for clearing. Incase of any pay in amount not paid by the client in time i.e., within 24 hours, the stocks will not be delivered to their demat account until the due is cleared.

As far as the receipts entry is concerned, all the receipts are entered in the Finance Module and the original receipt (Pre-printed) is handed over to the Client. All the receipts received by the Branches / Sub-Brokers are entered at their respective locations and then send the data to the Head Office through web along with a scanned copy of the Cheque / Demand Draft which is mandatory to authorize and give credit to the Client. Incase of non-receipt of the Scanned copy of the Cheque / Demand Draft, the receipt will not be considered and kept on hold till such time the scanned copy is received.

Payment of Pay-out

The Clients who have credit against their obligation account are paid on the basis of T + 3. The release of Pay Out amounts to clients is subject to deduction of any Shorts in the present settlement and any purchases made in the corresponding settlement. Based on the report given by the Clearing Department, the value of short deliveries either Internal or Exchange Shorts are arrived with the last traded rate and deducted from their respective pay out amounts and the net pay out is considered for payment. Once the Auction for the Un-delivered Stock takes place at the exchange level in the Auction Market, the actual auction amount with all charges levied by the exchange will be debited to the Short Clients and the net pay out is arrived. The internal shorts are also debited to the respective clients with the value of the stocks bought in the market on the settlement day. The long clients are given a benefit of 1 % of the value of the stocks bought and the same will be debited to the short clients. All the pay outs are to be paid by way of crossed cheques/demand drafts to the clients. Apart from the Short values there are also deductions with regard to the Demat Charges payable by the client. Any releases from the client's margin account are also paid by way of crossed cheques / demand drafts.

The pay out amounts are calculated at the Head Office and the net pay out amount will be made available on the web for the purpose of online requests. All the clients who require the pay out have to make the online request either individually or through the Branch / Sub-Broker. All the requests made by the Clients / Branches / Sub-brokers are taken into consideration for payment. The pay out amounts of clients for which no requests are made will be transferred to the Client's Margin Account on the same day.

Settlement with Exchange

All the obligations are to be settled with the exchange on the basis of T + 2. Pay in amounts are directly deducted from the Broker's Clearing Account with the Bank and the Pay out amounts are directly credited to the same Clearing Account. The exchange also has a policy of collecting Early Pay In amount, if necessary incase of a huge pay in obligation. Exchange also collects the Short Deliveries Amount for the un-delivered stock as Security Shortage in a particular settlement on the basis of the closing prices of the previous day of the Settlement day. The Auction for the un-delivered Stock is conducted in the Auction market by the Exchange and the Auction Report will be sent to the Broker along with the Auction Square Up Debit / Credit statements. The Auction Square up Debit statement is a statement for the stocks which could not be bought in the Auction market and the value is decided with a price target of +/- of the present value and squared off. The Auction Square up Credit statement is a statement of stock bought by the client and could not be delivered by the exchange instead squared off with a value of consideration as per the exchange policy. The Security Shortage Amount, which is collected on the Settlement Day, will be credited back and the Exchange will collect the actual Auction Amount on the Settlement Day of the Auction. The Daily Funds Statement will be sent to the Broker through FTP and will be available to the Broker by the end of the day.

The dividends received from the companies for stocks, which are in the pool account, are distributed to the clients. The distribution is based on the report given by the Clearing Department according to the client holdings.

Bank Reconciliation of all the accounts is regularly done and we have to make sure that there are no outstanding amounts.

The sharing of Brokerage to the sub-brokers is done on a periodical basis of every 15 days. The brokerage earned by the Sub-broker is given credit to his account for every 15 days and the payment will be made taking into consideration the default amounts of the clients pertaining to the Sub-broker.

Error Code policy

We maintain accuracy while placing orders of all Exchanges/Segments through NEAT and CTCL trading terminals. Human errors are inevitable on rare occasions, but all these erroneous codes are being committed due to typographical mistakes. The transactions executed other than actual code will be transferred to Error-code through Exchange on-line trade modification window during the market hours and corresponding quantity will be squared-off on behalf of actual code before market closes for the day.

Based on the net position of these transactions, the profit or loss will be settled between error-code and the actual code. In case the mistake is being committed by the operator himself or herself, corresponding quantity will be squared-off by the Member with anticipation of profit or loss.

As per the functional operations of the trading terminal, there will be a scope of happening above instances in NEAT only, but whereas CTCL trading terminal are much controlled while validating and processing the orders before execution.

The history of the above instances is being maintained in soft and hard copies for the future verifications during the audit trail.

Pre-funded Instruments / Electronic fund transfers Policy

This policy is in practice to maintain an audit trail while receiving funds through DD/PO/BC from the designated banks as per the convenience of the clients. Most of our fund transactions are being processed through Cheque only to the respective bank accounts of clients. Very occasionally we get funds through Demand Draft / Pay Order / Banker Cheque to meet the business requirements. We are also maintaining the details in attached format (Annexure-1) for every fund transfer being received from Demand Draft / Pay Order / Banker Cheque.

The following conditions are to be met while accepting funds through DD/PO/BC:

- If the aggregate value of pre-funded instruments is Rs. 50,000/- or more, per day per client, the Branch / Sub-broker / Authorised persons may accept the instruments only if the same are accompanied by the name of the bank account holder and number of the bank account debited for the purpose, duly certified by the issuing bank. The mode of certification may include the following:

* Certificate from the issuing bank on its letter head or on a plain paper with the seal of the issuing bank.

* Certificate copy of the requisition slip (portion which is retained by the bank) to issue the instrument.

* Certified copy of the passbook / bank statement for the account debited to issue the instrument.

* Authentication of the bank account – number debited and name of the account holder by the issuing bank on the reverse of the instrument.

And attached format (Annexure) in addition has to be maintained along with certified counter documents being received from the bankers. This is to maintain for the purpose of identify of each transaction and future reconciliation.

=== * * * ===

STEELEMENT OF FUNDS & SECURITIES POLICY

Running Account Authorization and Actual Settlement of Funds & Securities on monthly / quarterly basis:

The settlement of funds and / or securities shall be done within 1 working day of the payout, unless client specifically authorizes Steel City Securities Limited (SCSL) in writing to maintain a running account. Clients whose funds and securities are maintained on a running account basis have to be settled by members on a monthly / quarterly basis as per the client preference.

The periodicity for settlement of client funds and securities:

In case a client wishes to maintain a running account for its funds and securities with the Steel City Securities Limited (SCSL), the client has to authorize SCSL in writing to retain its funds and securities. Such authorization should also contain:

- preference of the client as to whether the settlement of funds and securities should be done on a monthly or quarterly basis

- a clause stating that the Client may revoke the authorization at any time (i.e. without notice)

Accordingly, the actual settlement of funds and securities shall be done by the member at least once in a calendar quarter or month, depending on the preference of the client.

Accounts need to be settled:

Steel City Securities Limited needs to settle the accounts of all clients who have opted for maintenance of running account instead of bill to bill settlement. However, in case of new clients who are registered at the end of a month / quarter, no settlement would be required to be done in the first month / quarter respectively in which the client is registered.

Balances need to be considered while settling funds and securities of clients:

Steel City Securities Limited has to settle clients "funds and securities" at least once in a calendar quarter or month.

Steel City Securities Limited needs to consider the EOD balance of funds and securities of clients across all segments of the Exchanges while settling the client accounts.

It is clarified that while settling client accounts, both funds and securities of clients need to be settled on the same day.

The value of funds / securities can retain while doing the settlement:

Clients having outstanding obligations on the settlement date, Steel City Securities Limited (SCSL) may retain the requisite funds / securities towards such obligations and may also retain the funds expected to be required to meet margin obligations for next 5 trading days, calculated in the manner specified by the exchanges.

Accordingly the following funds / securities may be retained by SCSL at the time of settlement

- Entire pay-in obligation of funds & securities outstanding at the end of day on date of settlement.

- funds / securities to the extent of value of transactions executed on the day of such settlement in the capital market.

- in derivative segment apart from margin liability as on the date of settlement, additional margins (maximum up-to 75% of margin requirement on the day of settlement)

An indicative format of retention statement is attached as Annexure 1. In case of any other format, members should ensure that the contents specified by the relevant circulars are covered in the retention statement.

Note:

a) While computing the value of securities, the closing rate for the trade date prior to the settlement date (T-1 day) should be considered after appropriate hair-cut viz. VaR margin rate applicable for the security in the Capital Market segment

b) In case the member applies hair cut in excess of VaR rate on a regular basis then such higher rate may be considered for determining the amount to be retained, provided the member has intimated the requirement of additional margins to the clients through the policy and procedures document and consistently through the daily margin statements issued to clients

c) No inter client adjustment can be done for the purpose of settling client accounts.

d) Obtaining of authorization from the clients to the effect that no settlement need be done for particular month(s) / quarter(s) is contradictory to the SEBI requirement and hence not permissible.

e) In case cheques issued in favor of the client, settlement will be deemed to have been done only if such cheque is cleared within a reasonable period.

f) In case of settlement done on trading holiday(s), T day to be considered for margins /turnover, etc., would be the previous trading day

g) Illiquid / volatile scrip's having VaR margin (hair cut) as 100% also need to be returned to the client if adequate securities are available with the member as per its risk management system.

Sending Statement of accounts for funds / securities:

Steel City Securities Limited is required to send to the client 'statement of accounts' containing an extract from the client ledger for funds, an extract from the register of securities displaying all receipts and deliveries of securities and a statement explaining the retention of funds and / or securities at the time of settlement.

The statement of accounts sent at the time of settlement may be sent in hard or in soft form as per the consent obtained from the client and POD / dispatch register / logs of email sent should be retained by the member.

Statement of accounts details sent at the time of settlement:

- Steel City Securities Limited could use any format for issue of statement of account at the time of settling client's accounts. However the statement should necessarily contain the following details:

- Transactions / MTM / margins debited and reversed / pay in and pay out of funds for the period from the date of last settlement done till the current settlement date.

- Security wise pay in pay out / securities retained as margin / securities pledged for the period from the date of last settlement done till the current settlement date.

- Closing balance of funds / securities available with the member on the date of settlement an error reporting clause giving clients not less than 7 working days from the date of receipt of funds / securities or statement, to bring any dispute arising from the statement of account or settlement so made to the notice of the member.

- A clause intimating the client that the client has provided a running account authorization which can be revoked at any time.

- In addition to the statement of account for funds members also need to provide to their clients a statement explaining the retention of funds / securities.

SCSL required to sent statement of accounts for funds / securities at the end of quarter in addition to the statement sent at the time of quarterly / monthly settlement:

In case Steel City Securities Limited has done monthly / quarterly settlement of client accounts and has sent statement of accounts for funds & securities as well as retention statement to the clients at the time of settlement as a part of settlement process, it would be considered adequate compliance for the purpose of sending quarterly statement of accounts for funds / securities for such clients provided statement of accounts (issued at the time of settlement) is sent on a regular basis to clients.

However, for clients whose settlement is not required to be done (e.g. Clients maintaining bill to bill pay in and pay out), SCSL is required to send statement of accounts for funds / securities at the end of quarter.

Statement of account required to be issued in case no trades are done by clients in the quarter / month:

In case a client has not traded during the quarter / month and SCSL does not hold any funds or securities for the client at any point of time during the quarter / month for which settlement needs to be done, then SCSL may decide not to issue statement of account to the client.

Settlement need not be done in the following circumstances:

Periodic settlement as per the above mentioned rules is not required to be done in the following cases:

a) Clients settling trades through “custodians”

b) Clients availing margin trading facility (to the extent of funds / securities relating to margin trading facility used by client)

c) Margin received in the form of Bank Guarantees and Fixed Deposit Receipts which are created by clients

d) Clearing members who are clearing trades of custodial participants / trading members

This policy is approved by the management and shall be followed by the concerned departments to meet the compliance /guidelines of SEBI and Exchanges.

Retaining period of Funds and Securities as per SCSL business rules while settling the funds and securities during the quarter for inactive clients

With respect to SEBI and Exchange guidelines and SCSL management committee directions, the retaining period of funds and securities being followed as per the below validations till further modification of Steel City Securities Limited business rules:

- In view of the business continuity and to ensure the sincere service front to our esteemed clients/investors, Steel City Securities Limited has decided to retain the funds up to Rs. 500/- (Five Hundred only) rupees, which will be settled in the ensuing quarter by sending an account payee cheque to the client's address as declared in the KYC document. In case the cheque gets returned, his account will be freeze by the SCSL.

There may be valid reasons for funds to freeze the account :

- Client is not traceable as per KYC details submitted
- Cheque delivered but not presented in the bank (within validity period of three months)
- Account is closed.
- Rejection of online transactions through NEFT/RTGS.

There may be valid reasons for securities to freeze the account :

- DEMAT account is closed
- DEMAT account is suspended due to non-submission of PAN details
- DEMAT account is suspended due to transmission
- ISIN is suspended

Funds retaining less than or equals to Rs. 500/-

- SCSL is retaining funds <= Rs. 500 towards recovery of any unpaid Transaction charges and DMAT charges etc. for both active and inactive clients.

- SCSL will not retain funds or securities without any intention other than mandatory recoveries.

While settling the Funds and Securities in a calendar quarter:

Clients having more than Rs. 500/- outstanding credit balance of funds / securities and not remitted to their respective client Bank / DEMAT account due to:

- Client is not traceable as per KYC details submitted.
- Cheque delivered but not presented in the bank (within validity period).
- Bank / Demat account is closed.
- Bank / Demat account is changed, which is not updated in the KYC.
- Rejection of online transactions through NEFT/RTGS.
- DEMAT account is suspended due to non-submission of PAN details.
- DEMAT account is suspended due to transmission.
- ISIN is suspended.

With effect to all the above instances including several communications, Steel City Securities Limited (SCSL) will wait till 3rd quarter from the date of settlement while transferring the unrealized funds / securities to ESCROW Account which is exclusively maintained to safe guard the investor's assets.

In the event of re-identification of client and requested for the payout from the outstanding credit balances of funds / securities, Steel City Securities Limited (SCSL) has to obtain a prior approval from the Management to release the funds / securities from ESCROW account based on the authentication (with valid proof of identity) of respective client.

This ESCROW account is operated with authorized signatories of the Management to prevent from the mis-utilization of investor's assets in any circumstances.

==== * * * ===