

Regulation of the Shenzhen Stock Exchange on the Access of Members and Other Entities to Its Trading System

(Ver 1.02)



Shenzhen Stock Exchange

March 2020

Document Description

Document name	Regulation of the Shenzhen Stock Exchange on the Access of Members and Other Entities to Its Trading System	
Description	This document sets for policies allowing members and other relevant entities to access the Shenzhen Stock Exchange's trading system.	
Note for English Version	This translation version of the document is issued by SSIC and acted as a reference only, please take the original version in Chinese on SZSE official website as standard.	
Revision history		
Date	Version	Revision description
May 16, 2017	Ver 1.00	Created documents.
February 8, 2018	Ver 1.01	Improved application security and management specifications.
March 17, 2020	Ver 1.02	<ol style="list-style-type: none"> 1. Managed the gateway monitoring as the access terminal; 2. Improved network access specifications, clarified the specific access requirements of futures companies, and emphasized collaborative configuration of access terminals to avoid line failures; 3. Systematically clarified information security specifications; 4. Clarified follow-up measures for violations, such as emergency response measures.

Table of Contents

I. Introduction	1
II. Application Management	1
III. Communication Network Access Management	2
IV. Information Security Specifications	2
V. Others	4

Regulation of the Shenzhen Stock Exchange on the Access of Members and Other Entities to Its Trading System

I. Introduction

In order to regulate the access of members and other relevant entities to the trading system of the Shenzhen Stock Exchange (hereinafter referred to as the “SZSE”) and ensure the safe operation of securities market transactions and related technical systems, SZSE has formulated the Regulation in accordance with the *Administrative Measures for Information Security Assurance for the Securities and Futures Industry*, the *Administrative Measures for Information Technology of Securities Fund Operators*, the *Rules of the Shenzhen Stock Exchange on Member Management* and industry self-regulation standards.

II. Application Management

1. Members and other relevant entities can only conduct business through application software licensed by SZSE or an agency authorized by SZSE. The application software version used shall comply with SZSE’s requirements and the application software version used shall be upgraded in a timely manner as required by SZSE.
2. Access terminals (including transaction gateways, market data gateways, file gateways, trading terminals, gateway monitoring, the same below) used by members and other relevant entities for transactions, market data and other services shall be based on the Guidelines of the Shenzhen Stock Exchange on Gateway Deployment and Access to ensure the high availability, integrity and security of the application system.
3. Members and other relevant entities shall evaluate the application software before installing it on the access terminal and maintain the evaluation records. A software list shall be prepared for the application software installed on the access terminal, and evaluation records and software lists shall be reported to SZSE. When the list of software installed on the access terminal changes, the assessment record and software list shall be reported to SZSE within five working days after the change. The format of the report evaluation record and software list is defined by the members and other relevant units themselves. They shall at least include the name and contact number of the person in charge of the report and the operating system version of the access terminal) and be sent by email to sseyxb@szse.cn.
4. The software and hardware change management records , all local and remote operation information, and log information of the operating system and application softwares of the access terminals must be saved, strictly prohibited from deletion and tampering, and kept for no less than one year.
5. The trading gateway, market data gateway, and file gateway shall not be logged in repeatedly. The same gateway number is only allowed to log in to transaction and related systems once at the same time. If hot standby is required, different gateway numbers shall be used.

III. Communication Network Access Management

1. Members must have two or more centralized operation centers that can backup each other, with access terminals and networks configured to access SZSE's trading system access services.
2. Members and other relevant entities must have network access lines from different carriers (including hosted access) and access SZSE's main and backup data centers respectively. Through the collaborative configuration of the application layer and network layer, it shall be ensured that business can continue to operate normally in the event of a single line or single carrier failure, and regular drills shall be conducted.
3. The communication network access of members and other relevant entities for centralized trading and market data business shall meet the following requirements:
 - The bandwidth of ground communication lines shall meet the minimum requirements: 10 Mbps for members, and 6 Mbps for fund companies, asset management companies, insurance companies and futures companies, etc;
 - During network debugging and after being put into operation, routing network (3 layers) ports must be used for the interface with SZSE, and switching (2 layers) ports are not allowed;
 - In addition to ground communication lines, there shall be at least one high-speed one-way satellite used as a backup for ground market conditions, and high-speed two-way satellites can be used as backup lines for transaction communication in extreme situations.
4. When a member's centralized operation center is hosted in the Data Center of Shenzhen Securities Communication Co., Ltd., mutually redundant communication lines shall be used to access the trading market custody network.
5. Members and other relevant entities using satellite access must abide by relevant national laws and regulations, keep in touch with the local radio management department, apply for radio station licenses, and report relevant information to the local radio management department.
6. In order to ensure the normal operation of transactions and related businesses, members and other relevant entities are obliged to cooperate with SZSE and entities authorized by SZSE in the upgrading, construction, and testing of communication networks.

IV. Information Security

1. When members and other relevant entities construct, operate, and maintain access terminals and networks connected to SZSE's trading and related systems, they shall comply with the requirements of "Transaction and related system management" in the Rules of the Shenzhen Stock Exchange on Member Management.
2. Shenzhen Securities Communication Network is an industry-specific network. After members and other relevant entities access the communication network, the access

terminals shall follow the following rules:

- The IP address of the access terminal (including the IP address after NAT address translation) must not be directly exposed to the Internet and other public networks;
- There shall be effective identification measures, including identification and authentication for logged in users;
- Effective access control measures shall be implemented, such as configuring access control policies by authorized subjects, which specify access rules for subjects to objects; The granularity of access control shall reach the user level or process level as the subject, and the file and database table level as the object;
- There shall be effective intrusion prevention measures, including following the principle of minimum installation, only installing necessary components and applications, etc.;
- The integrity of the application software accessed to SZSE on the access terminal and the security of data transmission shall be ensured. The damage to the integrity of the software itself, runtime memory data, and network data packets through memory injection, packet tampering, or other means must be avoided;
- It is not allowed to affect the operation of SZSE's application software through direct or indirect means, including the measurement of software, hardware and network environment, nor is it allowed to interfere with the normal transmission of data packets of SZSE's application software on the network through direct or indirect means.

3. After members and other relevant entities access the Shenzhen Securities Communication Private Network, the interconnected network equipment and the network equipment connected to the access terminal shall comply with the following rules:

- The network equipment must not be directly interconnected with the Internet and other public networks;
- Access control shall be strengthened for the network borders and important network nodes, and the principle of least authority shall be followed;
- Access control based on application protocols and application content shall be implemented for the data flow in and out of the network;
- There shall be the ability to detect and respond to attacks and intrusions, which can detect, prevent, or limit network attack behaviors initiated from both internal and external sources at critical network nodes. When an attack is detected, the attack source IP, attack type, attack target, and attack time shall be recorded, and an alarm shall be triggered when a serious intrusion occurs;
- It is forbidden to scan the IP address of the trading system server of SZSE (including the IP address after NAT address translation).

4. As an important part of the Shenzhen Securities Communication Private Network, members and other relevant entities shall follow the following rules in daily operations and management:

- Centralized management shall be carried out for security policies, malicious codes, patch upgrades and other security-related matters;
- A specific management area shall be allocated to manage, control and centrally monitor all network devices, servers, security devices or security components distributed from the access terminal to the Shenzhen Securities Communication Private Network;
- Audit data scattered on network borders, important network nodes, and various devices shall be collected and summarized, and various security events that have occurred shall be identified, analyzed and alerted.

5. For systems that have completed network security level protection classification filings, level protection evaluation work shall be carried out regularly.

V. Others

1. SZSE is responsible for the interpretation of the Regulation .
2. Members and other relevant entities shall promptly report any abnormal behavior that poses security risks to SZSE's trading system. If any concealment or delayed reporting of abnormal information is found and the system is used as a springboard to attack SZSE's trading system, once verified, such behavior will be considered a violation of the Regulation.
3. According to the *Basic Requirements for Network Security Level Protection*, when SZSE's trading system faces major security risks such as cyber attacks, SZSE may take emergency measures such as suspending network access of members and other relevant entities.
4. According to the relevant provisions of the *Rules of the Shenzhen Stock Exchange on Member Management*, SZSE can supervise and inspect the access terminals of members and other relevant entities.
5. Members and other relevant entities that fail to meet or violate the Regulation will be subject to corresponding self-regulatory measures or disciplinary sanctions in accordance with the *Rules of the Shenzhen Stock Exchange on Member Management*.
6. The Regulation shall come into effect from the date of release.
7. Contact for technical issues:

(0755) 82083510 (access terminal software registration and usage)

(0755) 83182222 (network access)