(UNOFFICIAL TRANSLATION)

Readers should be aware that only the original Thai text has legal force and that this English translation is strictly for reference. Thailand Futures Exchange Public Company Limited cannot undertake any responsibility for its accuracy nor be held liable for any loss or damages arising from or related to its use.

Security Standards for Systems Connected with TFEX Trading System

Whereas the Thailand Futures Exchange Public Company Limited (TFEX) recognizes the importance of the systems connected with the trading system of TFEX, which may affect the overall system security, TFEX hereby stipulates security standards for implementation and submission of details to TFEX upon request.

1. Physical and Environment Security

1.1 Secure Areas

To prevent unauthorized access to the secure areas in the computer room, which made lead to damage, interruption or interference to the property of the entity, there should be:

- area separation;
- access control by allowing entry and exit to authorized persons only;
- the recording of persons accessing the secure areas and the reasons for access each time;
- the installation of a standardized security system, for instance, use of an access control card for entry and exit of the computer room, or the provision of 24-hour access control officers; and
- implementation of guidelines for maintenance, prevention, and alerts for threats, for instance disruptions, fire, flood, earthquake, explosion, insurrection, or other manmade or natural disasters.

1.2 Equipment Security

Computer equipment and networks must be installed in an area which is subject to sufficient security, including prevention of loss, damage, theft, or unauthorized exposure, and any act which may disrupt or interrupt the operations.

- There must be a mechanism to prevent the failure of the system and support equipment, such as an electrical backup system, fire control system, temperature control system, and backup communication line system.
- The equipment must receive maintenance on a regular basis to ensure constant operation and to keep it in good working order.

2. Operations Management

These provisions set forth the policies, responsibilities, confidentiality obligation, and operation procedures to ascertain correct and safe operations, including user authentication, and user authorization. An operation log must be recorded and available for retroactive inspection back to a reasonable point in the past. The log must contain data which can specify the source, destination, date, time, user, operational data, or other significant information. In the case of the trading system or the clearing system, the details on the trading or the settlement must be clear enough for inspection.

2.1 Network Security

- Type of services, including the time of use of the security equipment and all kinds of connected network equipment must be specified and determined in accordance with actual use.
- System access security measures, for example, firewall, anti-virus, anti-spyware, anti-sniffing or anti-pilfering systems. Patch management must be available.
- Data on the routing protocols of the system must be properly encrypted.

2.2 System Security

- Safe procedures for access to or use of the system must be available.
- Every system must provide services only as necessary for use.
- System access security measures, for example, firewall, anti-virus, anti-spyware, anti-sniffing or anti-pilfering systems. Patch management, must be available.
- Use and event logs of the system must be recorded for retroactive inspection and kept for a reasonable time, for example, records on user access, use of server and database

2.3 Application Security

- Access to data and functions of applications must be restricted only to authorized persons and separated by types of users.
- A measure or technology which enables inspection and authentication of the identity of an authorized person, for example, user authentication and password, must be available
- A measure or technology which can exactly and properly identify the identity of order submitters, for example a PIN, or ID, must be available
- Warning messages sent to users must fully and clearly specify the risks which may arise from their actions.

3. User ID and Password Management

User ID and passwords include any other technology used for identification, such as a PIN, or ID. Such technologies play a important role in the control of access to the system, network, or applications. Therefore, the system or the management system must be sufficiently secured as follows:

- the ability to use only one (1) user login per session or as the TFEX deems appropriate;

- the length and characters of a password must be sufficiently secure (if a PIN, or ID, is used, its length must be sufficiently secure), and the output must not be shown in clear text;
- the password must be changed at appropriate intervals;
- the storage of a password in any system or equipment must be encrypted;
- in the event of an invalid login attempt, the login or password of any user must be locked immediately;
- the procedures for delivery of the User ID and password should be sufficiently secured, and users are informed of how to keep their password confidential, to ensure that they recognize the importance of security, for example, suggestion that a highly complicated password be used, that the password should not be disclosed to other persons, that logging out is necessary every time a user does not use the system, and information on possible risks in keeping the password in the computer or system.

4. Business Continuity Management

To prevent any disruption or interruption to business operations due to a failure of, or disaster to, security and performance of the information system, and to ensure system recovery within a reasonable time:

- a risk assessment with respect to events and sufficient measures to ensure operation continuity must be made, and such measures must be managed, improved and tested on a regular basis by specifying requirements relating to security as are necessary; and
- a back up for data, systems and applications must be available and kept for a reasonable period at a place other than the principal office of the entity, and the data must be immediately retrieved for use upon any disruption.