

**BỘ TÀI CHÍNH
ỦY BAN CHỨNG KHOÁN
NHÀ NƯỚC**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

Số: 379/QĐ-UBCK

Hà Nội, ngày 03 tháng 6 năm 2021

QUYẾT ĐỊNH

**BAN HÀNH TIÊU CHUẨN CƠ SỞ KỸ THUẬT HỆ THỐNG CÔNG NGHỆ THÔNG TIN
TRONG HOẠT ĐỘNG CUNG CẤP DỊCH VỤ GIAO DỊCH CHỨNG KHOÁN TRỰC
TUYẾN TRÊN THỊ TRƯỜNG CHỨNG KHOÁN**

CHỦ TỊCH ỦY BAN CHỨNG KHOÁN NHÀ NƯỚC

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật Chứng khoán ngày 26 tháng 11 năm 2019;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật Tiêu chuẩn và quy chuẩn kỹ thuật ngày 29 tháng 6 năm 2006;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 155/2020/NĐ-CP ngày 31 tháng 12 năm 2020 của Chính phủ quy định chi tiết thi hành một số điều của Luật Chứng khoán;

Căn cứ Quyết định số 48/2015/QĐ-TTg ngày 08 tháng 10 năm 2015 của Thủ tướng Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ủy ban Chứng khoán Nhà nước trực thuộc Bộ Tài chính;

Căn cứ Thông tư số 21/2007/TT-BKHCN ngày 28 tháng 9 năm 2007 của Bộ trưởng Bộ Khoa học và Công nghệ hướng dẫn xây dựng và áp dụng tiêu chuẩn;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 134/2017/TT-BTC ngày 19 tháng 12 năm 2017 của Bộ trưởng Bộ Tài chính hướng dẫn giao dịch điện tử trên thị trường chứng khoán;

Căn cứ Thông tư số 73/2020/TT-BTC ngày 07 tháng 8 năm 2020 sửa đổi, bổ sung một số điều của Thông tư số 134/2017/TT-BTC ngày 19 tháng 12 năm 2017 của Bộ trưởng Bộ Tài chính hướng dẫn giao dịch điện tử trên thị trường chứng khoán;

Theo đề nghị của Cục trưởng Cục Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Tiêu chuẩn cơ sở kỹ thuật hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán, cụ thể như sau:

- Tên tiêu chuẩn: Tiêu chuẩn cơ sở kỹ thuật hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán.

- Ký hiệu: TCCS 01:2021/UBCK.

- Quy chuẩn kỹ thuật Quốc gia tham chiếu: TCVN 11930:2017 công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ; TCVN 9250:2012 Trung tâm dữ liệu - yêu cầu về hạ tầng kỹ thuật viễn thông.

Điều 2. Trách nhiệm của các đơn vị:

1. Cục Công nghệ thông tin: Chủ trì hướng dẫn, kiểm tra, giám sát công ty chứng khoán, công ty quản lý quỹ, đại lý phân phối chứng chỉ quỹ và các tổ chức, cá nhân có liên quan đến hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán trong việc chấp hành Tiêu chuẩn này.

2. Vụ Quản lý kinh doanh chứng khoán và Vụ Quản lý các công ty quản lý quỹ và quỹ đầu tư chứng khoán - Ủy ban Chứng khoán Nhà nước, Sở Giao dịch chứng khoán, Trung tâm lưu ký chứng khoán Việt Nam: Phối hợp với Cục Công nghệ thông tin trong quá trình giám sát, kiểm tra các đối tượng chấp hành theo Tiêu chuẩn này.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký và bãi bỏ Quyết định số 106/QĐ-UBCK ngày 08/02/2010 của Chủ tịch Ủy ban Chứng khoán Nhà nước ban hành Quy định hướng dẫn về yêu cầu hệ thống công nghệ thông tin của công ty chứng khoán.

Điều 4. Chánh Văn phòng, Cục trưởng Cục Công nghệ thông tin, Vụ trưởng Vụ Quản lý kinh doanh chứng khoán, Vụ trưởng Vụ Quản lý các công ty quản lý quỹ và quỹ đầu tư chứng khoán, Thủ trưởng các đơn vị liên quan thuộc, trực thuộc Ủy ban Chứng khoán Nhà nước, Tổng Giám đốc Sở Giao dịch chứng khoán Việt Nam, Tổng Giám đốc Sở Giao dịch chứng khoán Hà Nội, Tổng Giám đốc Sở giao dịch chứng khoán thành phố Hồ Chí Minh, Tổng Giám đốc Trung tâm lưu ký chứng khoán Việt Nam, công ty chứng khoán, công ty quản lý quỹ, đại lý phân phối chứng chỉ quỹ và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

CHỦ TỊCH

Nơi nhận:

- Như điều 4;
- Lưu: VT, CNTT (150b).

Trần Văn Dũng

BỘ TÀI CHÍNH	TIÊU CHUẨN CƠ SỞ	TCCS 01:2021/UBCK
Ủy ban Chứng khoán Nhà nước	Tiêu chuẩn cơ sở kỹ thuật hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán.	Có hiệu lực từ Ngày tháng 6 năm 2021

(Ban hành kèm theo Quyết định số 379/QĐ-UBCK ngày 03/6/2021 của Chủ tịch Ủy ban Chứng khoán Nhà nước)

TCCS 01:2021/UBCK

TIÊU CHUẨN CƠ SỞ KỸ THUẬT HỆ THỐNG CÔNG NGHỆ THÔNG TIN TRONG HOẠT ĐỘNG CUNG CẤP DỊCH VỤ GIAO DỊCH CHỨNG KHOÁN TRỰC TUYẾN TRÊN THỊ TRƯỜNG CHỨNG KHOÁN

MỤC LỤC

MỞ ĐẦU

LỜI GIỚI THIỆU

CHƯƠNG I. QUY ĐỊNH CHUNG

- 1.1. Phạm vi điều chỉnh, đối tượng áp dụng
- 1.2. Giải thích thuật ngữ
- 1.3. Yêu cầu chung đối với hệ thống công nghệ thông tin

CHƯƠNG II. QUY ĐỊNH VỀ HẠ TẦNG KỸ THUẬT

2.1. Yêu cầu về hạ tầng kỹ thuật hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến

2.2. Yêu cầu đối với phòng máy chủ

2.3. Yêu cầu về nguồn điện

CHƯƠNG III. QUY ĐỊNH VỀ PHẦN MỀM VÀ DỮ LIỆU DỰ PHÒNG

3.1. Yêu cầu đối với phần mềm ứng dụng

3.2. Yêu cầu về lưu trữ và cung cấp dữ liệu cho cơ quan chức năng

3.3. Yêu cầu về sao lưu, phục hồi dữ liệu

CHƯƠNG IV. QUY ĐỊNH VỀ AN TOÀN BẢO MẬT

4.1. Yêu cầu về hệ thống máy chủ và hạ tầng mạng

4.2. Yêu cầu đối với phần mềm ứng dụng

4.3. Yêu cầu đối với trang thông tin điện tử

CHƯƠNG V. QUY ĐỊNH VỀ XÁC THỰC VÀ NHẬN DẠNG THIẾT BỊ ĐẶT LỆNH

5.1. Yêu cầu về sử dụng chữ ký số và xác thực giao dịch

5.2. Yêu cầu về nhận dạng thiết bị đặt lệnh

CHƯƠNG VI. QUY ĐỊNH VỀ NHÂN SỰ QUẢN LÝ HỆ THỐNG CÔNG NGHỆ THÔNG TIN

MỞ ĐẦU

Tiêu chuẩn cơ sở TCCS 01:2021/UBCK quy định về tiêu chuẩn kỹ thuật hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán do Cục Công nghệ thông tin - Ủy ban Chứng khoán Nhà nước biên soạn.

TCCS 01:2021/UBCK được xây dựng trên cơ sở tham khảo các bộ tiêu chuẩn quốc gia, các văn bản quy định về hệ thống công nghệ thông tin và có điều chỉnh, sửa đổi, bổ sung để phù hợp với các quy định về ứng dụng công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán như sau:

- TCVN 11930:2017 công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;
- TCVN 9250:2012 Trung tâm dữ liệu - yêu cầu về hạ tầng kỹ thuật viễn thông;
- Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;
- Thông tư số 134/2017/TT-BTC ngày 19 tháng 12 năm 2017 của Bộ trưởng Bộ Tài chính hướng dẫn giao dịch điện tử trên thị trường chứng khoán.
- Thông tư số 73/2020/TT-BTC ngày 07 tháng 8 năm 2020 sửa đổi, bổ sung một số điều của Thông tư số 134/2017/TT-BTC ngày 19 tháng 12 năm 2017 của Bộ trưởng Bộ Tài chính hướng dẫn giao dịch điện tử trên thị trường chứng khoán.

LỜI GIỚI THIỆU

Tiêu chuẩn cơ sở TCCS 01:2021/UBCK quy định về tiêu chuẩn kỹ thuật hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán quy định yêu cầu chi tiết về hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán, gồm các nhóm nội dung sau:

- Quy định chung.
- Quy định về hạ tầng kỹ thuật.
- Quy định về phần mềm và dữ liệu dự phòng.
- Quy định về an toàn bảo mật.
- Quy định về xác thực và nhận dạng thiết bị đặt lệnh
- Quy định về nhân sự quản lý hệ thống công nghệ thông tin.

Hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán phải bảo đảm đáp ứng quy định tại Thông tư 134/2017/TT-BTC ngày 19/12/2017 của Bộ trưởng Bộ Tài chính hướng dẫn giao dịch điện tử trên thị trường chứng khoán (sau đây gọi là Thông tư 134/2017/TT-BTC), Thông tư số 73/2020/TT-BTC ngày 07/8/2020 sửa đổi, bổ sung một số điều của Thông tư số 134/2017/TT-BTC ngày 19/12/2017 của Bộ trưởng Bộ Tài chính hướng dẫn giao dịch điện tử trên thị trường chứng khoán (sau đây gọi là Thông tư 73/2020/TT-BTC) và các nội dung hướng dẫn tại tiêu chuẩn này.

Chương I.

QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh, đối tượng áp dụng

1.1.1. Quy định này hướng dẫn chi tiết về tiêu chuẩn kỹ thuật đối với hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến trên thị trường chứng khoán.

Hoạt động trao đổi thông tin điện tử trên thị trường chứng khoán và các hoạt động khác liên quan đến giao dịch điện tử trên thị trường chứng khoán được thực hiện theo các quy định tại Thông tư 134/2017/TT-BTC ngày 19 tháng 12 năm 2017 của Bộ trưởng Bộ Tài chính hướng dẫn giao dịch điện tử trên thị trường chứng khoán, Thông tư số 73/2020/TT-BTC ngày 07 tháng 8 năm 2020 sửa đổi, bổ sung một số điều của Thông tư số 134/2017/TT-BTC và quy định của pháp luật về giao dịch điện tử trong hoạt động tài chính.

1.1.2. Đối tượng áp dụng: công ty chứng khoán, công ty quản lý quỹ, đại lý phân phối chứng chỉ quỹ và các tổ chức, cá nhân có liên quan đến hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến.

1.2. Giải thích thuật ngữ

1.2.1. *Hệ thống công nghệ thông tin* bao gồm các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu, hệ thống mạng viễn thông, mạng Internet, mạng máy tính, trang thông tin điện tử để phục vụ giao dịch chứng khoán trực tuyến.

1.2.2. *Chủ quản hệ thống thông tin phục vụ giao dịch chứng khoán trực tuyến* (sau đây gọi tắt là “*chủ quản hệ thống thông tin*”) là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp hệ thống thông tin phục vụ hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến.

1.2.3. *Vùng mạng biên* là vùng mạng được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác.

1.2.4. *Vùng DMZ (demilitarized zone)* là vùng mạng được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet.

1.2.5. *Vùng mạng nội bộ (LAN - local area network)* là vùng mạng được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị mạng khác của người sử dụng vào hệ thống.

1.2.6. *Dự phòng nóng* là khả năng hoạt động thay thế chức năng của thiết bị khi xảy ra sự cố mà không làm gián đoạn hoạt động của hệ thống.

1.2.7. *Máy chủ (Server) chuyên dùng* là một máy tính được thiết kế cho phép hoạt động 24/7; hỗ trợ dự phòng và thay nóng bộ cấp nguồn, ổ đĩa cứng được kết nối với một mạng máy tính hoặc Internet, có địa chỉ IP tĩnh, có năng lực xử lý cao và trên đó có thể cài đặt các phần mềm để phục vụ cho các máy tính khác truy cập để yêu cầu cung cấp các dịch vụ và tài nguyên.

1.2.8. *Mã hóa một chiều* là phương pháp mã hóa sử dụng hàm băm (Hash function) để biến một chuỗi thông tin thành một chuỗi có độ dài nhất định (chuỗi hash) không thể giải mã.

1.2.9. *Thông tin định danh thiết bị đặt lệnh* là thông tin gắn với mỗi thiết bị dùng để nhận dạng thiết bị khi thực hiện giao dịch chứng khoán trực tuyến.

1.2.10. *Lần thực hiện giao dịch* là lần nhà đầu tư đăng nhập hệ thống giao dịch chứng khoán trực tuyến để thực hiện các lệnh giao dịch chứng khoán trực tuyến.

1.2.11. *SSL (Secure Sockets Layer)* là tiêu chuẩn công nghệ cho phép thiết lập kết nối được mã hóa an toàn giữa máy chủ web và trình duyệt của người dùng, bảo đảm tính riêng tư và toàn vẹn của dữ liệu được truyền nhận giữa máy chủ web và trình duyệt của người dùng.

1.2.12. *Địa chỉ vật lý của thiết bị đặt lệnh (còn gọi là địa chỉ MAC - Media Access Control)* là mã duy nhất được gán bởi nhà sản xuất dùng để nhận dạng thiết bị.

1.2.13. *Xác thực sinh trắc học (Biometric)* là công nghệ sử dụng những thuộc tính vật lý, đặc điểm sinh học riêng của mỗi cá nhân như vân tay, khuôn mặt, móng mắt, tĩnh mạch,... để nhận diện, xác thực bảo mật.

1.3. Yêu cầu chung đối với hệ thống công nghệ thông tin

1.3.1. Hệ thống công nghệ thông tin bảo đảm đáp ứng được yêu cầu về dịch vụ, hạ tầng kỹ thuật, an ninh bảo mật và lưu trữ dữ liệu theo quy định tại Thông tư 134/2017/TT-BTC, Thông tư 73/2020/TT-BTC và phù hợp với quy định khác tại các văn bản quy phạm pháp luật chuyên ngành về chứng khoán và thị trường chứng khoán.

1.3.2. Hệ thống công nghệ thông tin phải được thiết kế có dự phòng; có khả năng phục hồi nhanh chóng khi xảy ra sự cố, sẵn sàng cung cấp dịch vụ giao dịch chứng khoán và cung cấp thông tin cho khách hàng; bảo đảm khả năng mở rộng, nâng cấp trong tương lai và bảo đảm tối ưu hoá năng lực xử lý thông tin của mạng máy tính.

1.3.3. Chủ quản hệ thống thông tin ban hành quy định về an toàn, an ninh thông tin, xử lý sự cố; quy định về trách nhiệm cập nhật, vá lỗi, khắc phục lỗ hổng bảo mật của hệ thống công nghệ thông tin; xây dựng kế hoạch định kỳ kiểm tra, rà soát về an toàn an ninh thông tin trong quá trình vận hành hệ thống.

Chương II.

QUY ĐỊNH VỀ HẠ TẦNG KỸ THUẬT

2.1. Yêu cầu về hạ tầng kỹ thuật hệ thống công nghệ thông tin trong hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến

2.1.1. Chủ quản hệ thống thông tin phải sử dụng máy chủ chuyên dùng cho hệ thống công nghệ thông tin phục vụ hoạt động cung cấp dịch vụ giao dịch chứng khoán trực tuyến. Phần mềm ứng

dụng và các dịch vụ liên quan đến hoạt động giao dịch của các nhà đầu tư phải được duy trì hoạt động trên các máy chủ. Không sử dụng máy tính cá nhân đóng vai trò máy chủ và không sử dụng chung máy chủ của các đơn vị khác.

2.1.2. Hệ thống đường truyền kết nối với Sở giao dịch chứng khoán, Trung tâm lưu ký chứng khoán Việt Nam phải có dự phòng nóng.

2.1.3. Máy chủ cài đặt phần mềm giao dịch chứng khoán, máy chủ cơ sở dữ liệu và trang thiết bị công nghệ thông tin chuyên dùng cho hệ thống giao dịch chứng khoán trực tuyến phải có dự phòng.

2.2. Yêu cầu đối với phòng máy chủ

2.2.1. Phòng máy chủ phải được bố trí bảo đảm đủ điều kiện cho các thiết bị hoạt động: đặt ở nơi khô ráo, tránh ánh nắng trực tiếp, tránh nguy cơ cháy nổ hoặc nguồn nhiệt cao, tránh nước ngập và bảo đảm an toàn bảo mật.

2.2.2. Phòng máy chủ phải có nội quy và áp dụng các biện pháp bảo vệ, kiểm soát ra vào, cửa ra vào phải chắc chắn, có khả năng chống cháy, sử dụng ít nhất hai loại khóa khác nhau (khóa cơ, thẻ, mã số, sinh trắc học); có hệ thống camera giám sát, ghi lại thông tin ra vào phòng máy chủ và mọi hoạt động tại các khu vực trong phòng máy chủ; hệ thống phải được quản lý tập trung và được theo dõi, giám sát 24/7, có nhật ký kiểm soát vào ra. Dữ liệu nhật ký camera phải được lưu trữ tối thiểu một (01) tháng; thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả.

2.2.3. Phòng máy chủ phải lắp đặt hệ thống cảnh báo cháy và chữa cháy tự động, chất chữa cháy là khí không gây ngạt cho nhân viên thao tác hoặc chưa kịp thoát ra, bảo đảm khi chữa cháy không làm hư hỏng thiết bị lắp đặt bên trong; có các hình thức phát tín hiệu cảnh báo cháy khác nhau (bằng âm thanh, ánh sáng...).

2.2.4. Có hệ thống chống sét trực tiếp và lan truyền; có hệ thống theo dõi, kiểm soát nhiệt độ và độ ẩm; có hệ thống điều hòa bảo đảm hoạt động liên tục. Hệ thống điều hòa không khí tại phòng máy chủ phải bảo đảm hoạt động liên tục và riêng biệt hoàn toàn với các hệ thống điều hòa khác trong tòa nhà.

2.2.5. Phòng máy chủ không được xây dựng cửa sổ, không được đặt các thiết bị không liên quan đến việc hỗ trợ phòng máy chủ (như hệ thống ống dẫn, hệ thống ống hơi,...) ở trong phòng máy chủ. Không được chạy ống thoát nước và ống dẫn nước gần hoặc trực tiếp trên thiết bị trong phòng máy chủ.

2.2.6. Ban hành quy định quản lý, vận hành và sử dụng phòng máy chủ.

2.3. Yêu cầu về nguồn điện

2.3.1. Phòng máy chủ có tối thiểu một nguồn điện lưới và một nguồn điện máy phát. Có hệ thống chuyển mạch tự động giữa hai nguồn điện, khi cắt điện lưới, trong thời gian tối đa ba (03) phút

máy phát phải tự động khởi động cấp nguồn; Nguồn điện trong phòng máy chủ phải được bảo đảm ổn định, chống quá tải và phải đấu nối qua bộ cấp điện liên tục trực tuyến (UPS online) để cấp nguồn cho thiết bị, bảo đảm khả năng duy trì hoạt động của thiết bị trong thời gian tối thiểu 30 phút.

2.3.2. Nguồn điện dự phòng phải đủ tiêu chuẩn, công suất cho hoạt động bình thường của hệ thống công nghệ thông tin trong thời gian nguồn điện chính có sự cố.

Chương III.

QUY ĐỊNH VỀ PHẦN MỀM VÀ DỮ LIỆU DỰ PHÒNG

3.1. Yêu cầu đối với phần mềm ứng dụng

3.1.1. Phải thực hiện theo quy định của pháp luật hiện hành về bản quyền phần mềm. Giải pháp công nghệ để xây dựng phần mềm ứng dụng phải đáp ứng khả năng nâng cấp mở rộng, có khả năng kiểm soát các truy cập về thao tác nghiệp vụ trong giao dịch, bảo đảm thực hiện đúng quy trình. Phải có khả năng tự động kiểm tra dữ liệu nhập vào ứng dụng, bảo đảm dữ liệu được nhập vào chính xác và hợp lệ; có khả năng lưu vết các giao dịch và các tương tác của người dùng.

3.1.2. Trước khi đưa vào sử dụng phải được đặt tên, thuyết minh rõ xuất xứ, tính năng kỹ thuật và có tài liệu hướng dẫn cụ thể kèm theo như: phân tích thiết kế hệ thống, tài liệu yêu cầu người sử dụng, hướng dẫn sử dụng.

3.1.3. Hệ thống phần mềm giao dịch chứng khoán trực tuyến phải có tính năng giám sát người sử dụng như: tài khoản và thời gian truy cập vào hệ thống (giây:phút:giờ, ngày/tháng/năm); tài khoản và thời gian tạo ra dữ liệu, thời gian sửa dữ liệu cuối cùng, thông tin đăng nhập (tên tài khoản và thời gian đăng nhập/đăng xuất, các thao tác thực hiện trong thời gian đó), thông tin định danh thiết bị đặt lệnh.

3.1.4. Kiểm soát sự thay đổi của phiên bản phần mềm, quy trình vận hành; ghi chép lại các thay đổi, lập kế hoạch, thực hiện kiểm tra, thử nghiệm sự thay đổi, báo cáo kết quả và phải được phê duyệt của người có thẩm quyền trước khi áp dụng chính thức.

3.2. Yêu cầu về lưu trữ và cung cấp dữ liệu cho cơ quan chức năng

3.2.1. Dữ liệu giao dịch chứng khoán phải được lưu trữ tối thiểu mười (10) năm, bảo đảm giá trị pháp lý trong quá trình lưu trữ và bảo đảm các điều kiện quy định tại khoản 1 Điều 15 Luật giao dịch điện tử.

3.2.2. Dữ liệu giao dịch chứng khoán phải bảo đảm truy cập được, sử dụng được dưới dạng hoàn chỉnh khi cần thiết.

3.2.3. Trong trường hợp cần thiết, khi có yêu cầu của cơ quan chức năng, chủ quản hệ thống thông tin phải cung cấp đầy đủ, kịp thời dữ liệu giao dịch chứng khoán.

3.3. Yêu cầu về sao lưu, phục hồi dữ liệu

3.3.1. Chủ quản hệ thống thông tin có trách nhiệm xây dựng, triển khai và thực hiện nghiêm túc các quy trình về sao lưu, dự phòng, phục hồi hệ thống thông tin, dữ liệu, tệp cấu hình thiết bị; tổ chức thực hiện phục hồi dữ liệu khi cần thiết cho hệ thống công nghệ thông tin.

3.3.2. Phải lập danh sách các dữ liệu, phần mềm, tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, thông tin nghiệp vụ, các file ghi âm đặt lệnh cần được sao lưu, có phân loại theo mức độ quan trọng, thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

3.3.3. Dữ liệu của hệ thống giao dịch chứng khoán trực tuyến phải được sao lưu ra phương tiện lưu trữ ngoài (như băng từ, đĩa cứng, đĩa quang hoặc phương tiện lưu trữ khác) và phương tiện lưu trữ phải được bảo quản tách rời với khu vực sao lưu. Dữ liệu lưu trên các thiết bị lưu trữ phải được bảo vệ vật lý trong môi trường bảo mật và bảo đảm khôi phục thông tin, dữ liệu trong vòng hai mươi bốn (24) giờ kể từ khi phát sinh sự cố.

3.3.4. Cần tách biệt giữa sao lưu dữ liệu và sao lưu ứng dụng. Mọi ứng dụng được cài đặt hoặc xóa bỏ khỏi hệ thống thông tin đều cần được sao lưu vào hệ thống dự phòng, tách biệt khỏi hệ thống sao lưu dữ liệu. Dữ liệu phải được kiểm soát và đối chiếu sau khi sao lưu.

3.3.5. Việc sao lưu và phục hồi trang thông tin điện tử phải bảo đảm các yêu cầu sau: Trang thông tin điện tử phải được sao lưu toàn bộ, bao gồm cả phần mềm và cơ sở dữ liệu lưu nội dung thông tin. Trong trường hợp gặp sự cố, trang thông tin điện tử phải được phục hồi trong thời gian không quá hai mươi bốn (24) giờ kể từ khi xảy ra sự cố.

Chương IV.

QUY ĐỊNH VỀ AN TOÀN BẢO MẬT

4.1. Yêu cầu về hệ thống máy chủ và hạ tầng mạng

4.1.1. Sử dụng giải pháp phát hiện, ngăn chặn xâm nhập và ngăn chặn tấn công trực tiếp vào các thông tin quan trọng của hệ thống.

4.1.2. Hệ thống dịch vụ giao dịch chứng khoán trực tuyến được giám sát chặt chẽ; có khả năng phát hiện, cảnh báo về: Các giao dịch đáng ngờ, gian lận dựa vào việc xác định thời gian, tần suất giao dịch, khối lượng giao dịch, số lần xác thực sai quy định và các dấu hiệu bất thường khác; hoạt động bất thường của hệ thống; Các cuộc tấn công từ chối dịch vụ (DoS - Denial of Service), tấn công từ chối dịch vụ phân tán (DDoS - Distributed Denial of Service).

4.1.3. Sử dụng phần mềm chống virus, phần mềm chống phần mềm gián điệp trên tất cả các máy chủ, máy trạm và tại cổng kết nối với các mạng bên ngoài bao gồm cả các cổng kết nối tới các đối tác và Internet. Các phần mềm này phải có bản quyền, có nguồn gốc rõ ràng. Định kỳ cập nhật các bản vá lỗi phù hợp với hệ điều hành máy chủ, máy trạm, tường lửa, hệ thống ngăn chặn xâm nhập (IPS - Intrusion Prevention Systems) và các phần mềm hệ thống khác.

4.1.4. Sử dụng các giải pháp như: mạng riêng ảo, mã hóa các dữ liệu trên đường truyền, kiểm soát truy cập web nhằm giảm thiểu các nguy cơ mất an toàn cho các máy trạm khi truy cập web, ngăn chặn thư rác, tường lửa cho ứng dụng web. Việc truy cập hệ thống phải được phân quyền đến từng bộ phận, cá nhân sử dụng để bảo vệ các lớp thông tin khác nhau. Các máy chủ phải được cài đặt, cấu hình để hệ thống có thể lưu vết mọi xâm nhập.

4.1.5. Hệ thống mạng của các tổ chức cung cấp dịch vụ giao dịch chứng khoán trực tuyến phải được thiết lập tối thiểu gồm các phân vùng: vùng mạng nội bộ, vùng mạng biên, vùng DMZ.

4.1.6. Các phân vùng mạng phải có chính sách bảo mật cho từng vùng.

4.1.7. Chủ quản hệ thống thông tin phải có các biện pháp bảo đảm chỉ nhân sự được giao quản trị hệ thống có thể tiếp cận và vận hành các máy tính thực hiện công tác quản trị hệ thống; các máy tính thực hiện công tác quản trị hệ thống không được kết nối Internet.

4.1.8. Các máy trạm, đặc biệt là các máy tính trang bị cho cán bộ nghiệp vụ liên quan đến giao dịch chứng khoán phải có biện pháp an toàn bảo mật: niêm phong thùng máy và các cổng kết nối ngoại vi, cài đặt mật khẩu cho máy tính, thực hiện thu hồi quyền truy cập khi cán bộ chấm dứt hoặc thay đổi công việc.

4.1.9. Chủ quản hệ thống thông tin phải quy định rõ nhiệm vụ, quyền hạn và trách nhiệm của các đối tượng tham gia quản lý, sử dụng hệ thống công nghệ thông tin và dịch vụ cung cấp.

4.1.10. Xây dựng danh mục và xác định mức độ quan trọng của dữ liệu, trên cơ sở đó áp dụng các chính sách, giải pháp an ninh bảo mật phù hợp với mức độ quan trọng của từng loại dữ liệu.

4.1.11. Chủ quản hệ thống thông tin phải ký hợp đồng với các tổ chức được thuê thực hiện nâng cấp, bảo trì, sửa lỗi phần mềm, trong đó quy định chi tiết các nội dung công việc, dữ liệu, quy định rõ trách nhiệm của các bên liên quan. Bảo đảm an toàn bảo mật thông tin, dữ liệu của hệ thống giao dịch chứng khoán trực tuyến của công ty và thông tin, dữ liệu của nhà đầu tư.

4.2. Yêu cầu đối với phần mềm ứng dụng

4.2.1. Phần mềm ứng dụng phải bảo đảm có khả năng phân quyền theo chức năng đến từng người sử dụng. Mỗi người sử dụng được phân định rõ ràng về nhiệm vụ và quyền hạn. Người không được phân quyền không thể truy cập vào công việc của người khác. Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng.

4.2.2. Các phần mềm ứng dụng có chức năng giao dịch qua Internet phải có cơ chế xác thực người sử dụng và mã hóa dữ liệu trên đường truyền.

4.2.3. Khi cung cấp phần mềm ứng dụng giao dịch chứng khoán trực tuyến trên Internet phải áp dụng các biện pháp bảo đảm tính toàn vẹn của phần mềm.

4.2.4. Mật khẩu người sử dụng khi lưu trữ phải được mã hóa một chiều. Nghiêm cấm trao đổi mật khẩu người sử dụng dưới dạng văn bản không mã hóa (clear text), trừ trường hợp cung cấp trực tiếp cho khách hàng khi khách hàng đến làm thủ tục cấp mới hoặc cấp lại mật khẩu.

4.2.5. Phần mềm ứng dụng phải có các cơ chế:

- Yêu cầu người sử dụng thay đổi mật khẩu lần đầu tiên đăng nhập và định kỳ thay đổi;
- Thiết lập quy tắc đặt mật khẩu theo số lượng ký tự, loại ký tự; thiết lập thời gian yêu cầu thay đổi mật khẩu;
- Hạn chế số lần đăng nhập sai, có cơ chế cảnh báo và tạm thời khóa tài khoản người dùng nếu đăng nhập sai thông tin nhiều lần;
- Phần mềm giao dịch chứng khoán trực tuyến phải được thiết lập thời gian cho mỗi lần thực hiện giao dịch và thiết lập khoảng thời gian khách hàng không thao tác trên hệ thống để kích hoạt tính năng thoát (logout) khỏi hệ thống.

4.3. Yêu cầu đối với trang thông tin điện tử

4.3.1. Hệ thống máy chủ của trang thông tin điện tử phải được trang bị giải pháp giám sát việc thay đổi quyền điều khiển, giám sát sự thay đổi nội dung của trang thông tin điện tử.

4.3.2. Đối với những trang thông tin điện tử thực hiện giao dịch chứng khoán trực tuyến, phần nội dung giao dịch chứng khoán trực tuyến phải được tách riêng và đặt trên máy chủ riêng biệt. Các thông tin giao dịch, tài khoản và mật khẩu phải được mã hoá, bảo đảm bí mật cho khách hàng.

4.3.3. Trang thông tin điện tử phải được xác thực sử dụng chứng thư số SSL, phải được áp dụng các biện pháp bảo vệ nhằm ngăn chặn, chống sửa đổi trái phép, chống giả mạo.

Chương V.

QUY ĐỊNH VỀ XÁC THỰC VÀ NHẬN DẠNG THIẾT BỊ ĐẶT LỆNH

5.1. Yêu cầu về sử dụng chữ ký số và xác thực giao dịch

5.1.1. Khuyến khích nhà đầu tư lựa chọn sử dụng chứng thư số, chữ ký số của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng khi thực hiện lệnh giao dịch chứng khoán trực tuyến.

5.1.2. Hệ thống phần mềm giao dịch chứng khoán trực tuyến phải tích hợp giải pháp sử dụng chứng thư số, chữ ký số để nhà đầu tư xác thực danh tính và ký phiếu lệnh điện tử khi lựa chọn giải pháp này để thực hiện giao dịch.

5.1.3. Chủ quản hệ thống thông tin có thể tích hợp các giải pháp xác thực khác có độ an toàn tối thiểu phải tương đương giải pháp xác thực hai yếu tố trở lên (OTP, thẻ ma trận, sinh trắc học...).

Trường hợp sử dụng dịch vụ của bên thứ ba (đơn vị cung cấp giải pháp xác thực), phải có tối thiểu một yếu tố xác thực do chủ quản hệ thống thông tin quản lý.

5.1.4. Cơ chế xác thực theo lần thực hiện giao dịch:

- Trong mỗi lần thực hiện giao dịch, nhà đầu tư có thể thực hiện nhiều lệnh giao dịch; nhà đầu tư phải xác thực khi thực hiện lệnh giao dịch đầu tiên, không bắt buộc xác thực khi thực hiện các lệnh tiếp theo. Lần giao dịch kết thúc nếu sau một khoảng thời gian (do chủ quản hệ thống thông tin thiết lập) mà nhà đầu tư không tiếp tục thực hiện lệnh giao dịch.

- Thông tin xác thực của mỗi lần thực hiện giao dịch phải được gắn với tất cả các phiếu lệnh điện tử được khởi tạo trong lần thực hiện giao dịch đó, bảo đảm phù hợp với nội dung quy định về phiếu lệnh điện tử tại Thông tư 134/2017/TT-BTC và Thông tư 73/2020/TT-BTC.

5.2. Yêu cầu về nhận dạng thiết bị đặt lệnh

Hệ thống có thể truy cập các thông tin định danh thiết bị đặt lệnh như sau:

5.2.1. Đối với ứng dụng trên thiết bị di động hoặc trên máy tính:

- Ứng dụng trên thiết bị di động có thể truy cập thông tin như: Số IMEI, số Serial, WLAN MAC, số Android ID hoặc thông tin định danh duy nhất khác của thiết bị.

- Ứng dụng chạy trực tiếp trên máy tính với các hệ điều hành (Linux, Windows, MacOS,...) có thể truy cập thông tin địa chỉ MAC hoặc thông tin định danh thiết bị khác thông qua các API (Application Programming Interface) của hệ điều hành.

5.2.2. Đối với trình duyệt (cho thiết bị di động hoặc máy tính): Xây dựng công cụ mở rộng cho phép truy xuất thông tin nhận dạng thiết bị thông qua các API (ví dụ: plugin,...) để người dùng cài đặt lên trình duyệt khi có nhu cầu đặt lệnh qua website.

Chương VI.

QUY ĐỊNH VỀ NHÂN SỰ QUẢN LÝ HỆ THỐNG CÔNG NGHỆ THÔNG TIN

6.1. Nhân sự quản lý hệ thống công nghệ thông tin phải có lý lịch rõ ràng, trình độ chuyên môn phù hợp với vị trí công việc được phân công. Chủ quản hệ thống thông tin phải có chính sách thẩm tra, xác minh lý lịch của cán bộ quản lý và cán bộ kỹ thuật vận hành, chịu trách nhiệm tại các vị trí quan trọng của hệ thống thông tin như: Quản trị hệ thống, quản trị hệ thống an ninh bảo mật, vận hành hệ thống, quản trị cơ sở dữ liệu.

6.2. Hợp đồng tuyển dụng cán bộ công nghệ thông tin phải bao gồm cam kết bảo mật thông tin. Cam kết này phải bao gồm các điều khoản về trách nhiệm bảo đảm an toàn, bảo mật hệ thống thông tin trong và sau khi làm việc tại vị trí công việc được giao; điều khoản xử lý vi phạm và trách nhiệm bồi thường do vi phạm các quy định về an toàn bảo mật hệ thống công nghệ thông tin của cán bộ được tuyển dụng trong và sau khi làm việc tại vị trí công việc được giao.

6.3. Khi cán bộ, nhân viên công nghệ thông tin chấm dứt hoặc thay đổi vị trí công việc, phải có biên bản bàn giao tài sản công nghệ thông tin; thu hồi quyền truy cập hệ thống thông tin của cán bộ, nhân viên nghỉ việc hoặc thay đổi quyền truy cập hệ thống công nghệ thông tin của cán bộ, nhân viên phù hợp với công việc được thay đổi.

6.4. Chủ quản hệ thống thông tin thực hiện phổ biến và cập nhật các quy định về an toàn bảo mật công nghệ thông tin cho cán bộ, nhân viên tại đơn vị. Yêu cầu và kiểm tra việc thi hành các quy định về an toàn, bảo mật công nghệ thông tin của cá nhân, tổ chức thuộc đơn vị tối thiểu một (01) năm một (01) lần.

6.5. Những công việc quan trọng như cấu hình hệ thống an ninh mạng, thay đổi tham số hệ điều hành, cài đặt thiết bị tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập phải được thực hiện bởi ít nhất hai người hoặc phải có người giám sát./.